PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-051837
(43)Date of publication of application : 21.02.2003

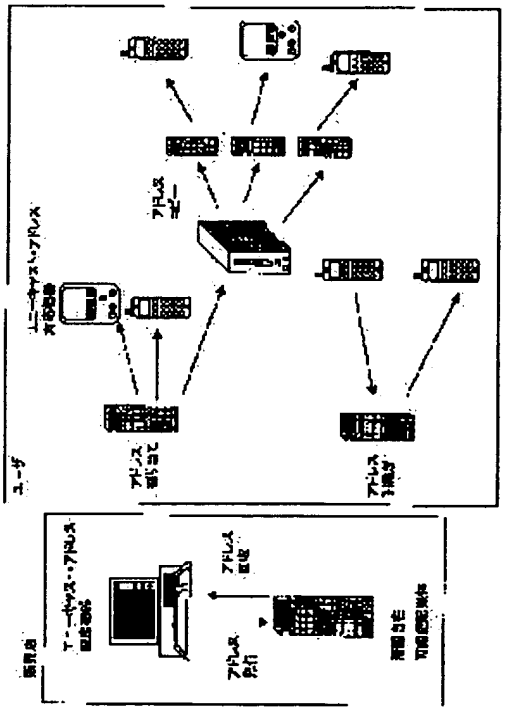
(51)Int.CI. H04L 12/56
// G06F 15/00

(21)Application number : 2001-239147
(22)Date of filing : 07.08.2001

(71)Applicant : SONY CORP
(72)Inventor : MIYOSHI HIROSHI
MIYAUCHI ATSUSHI

(54) ADDRESS MANAGEMENT SYSTEM, ANY-CAST ADDRESS SETTING PROCESSING UNIT, COMMUNICATION TERMINAL, INFORMATION STORAGE DEVICE, ADDRESS MANAGEMENT METHOD, AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an improved address management processing system utilizing a portable storage medium.
SOLUTION: Using a portable storage medium to distribute any-cast address can allow diversified communication terminals to utilize the any-cast address. Since the any-cast address is unchanged in spite of replacement of devices, IPv6 communication can be used for a service with high versatility such as a phone service. Further, the any-cast address can be used for an identifier unique to a user, and the any-cast address is useful for the infrastructure of a service compatible with each individual customer. Further, the any-cast address can be processed for movement, copy and return or the like, the any-cast address can be used circulatingly and the any-cast address can efficiently be utilized.



LEGAL STATUS
[Date of request for examination] 28.03.2003
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

JP 2003-051837

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The communication terminal which is the address managerial system which manages the address set as the communication terminal which performs communications processing, and serves as an address selection object, The portable mold storage which equips said communication terminal and stores the ENI cast address, It has the ENI cast address selection processor which publishes ENI cast address information as the address corresponding to this communication terminal, and said ENI cast address selection processor is subject [to authentication formation of a portable mold storage]. The portable mold storage which outputted ENI cast address information to said portable mold storage, and received said ENI cast address information Receiving ENI cast address information is stored in the memory in a portable mold storage, and it is contingent [on authentication formation with the connected communication terminal]. ENI cast address information is outputted to said communication terminal. Said communication terminal The address managerial system characterized by having the configuration which sets up the address included in the ENI cast address information which received from said portable mold storage as this ENI cast address corresponding to a communication terminal.
[Claim 2] The address included in said ENI cast address information is an address managerial system according to claim 1 characterized by being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[Claim 3] Said ENI cast address selection processor Electronic signature is added and outputted to the ENI cast address information stored in a portable mold storage a condition [authentication formation of a portable mold storage]. The portable mold storage which received said ENI cast address information and electronic signature The address managerial system according to claim 1 characterized by storing receiving ENI cast address information and electronic signature in the memory in a portable mold storage a condition [the check of there being no alteration of received data by verification of electronic signature].
[Claim 4] The address managerial system according to claim 1 which attribute information including utilization conditions is added and stored in the ENI cast address information stored in a portable mold storage, and is characterized by being the configuration that the electronic signature for alteration verification was added to this attribute information.
[Claim 5] The address managerial system according to claim 1 characterized by to be the configuration which the attribute information which includes utilization conditions in the ENI cast address information stored in a portable mold storage is added and stored, adds the electronic signature by the device which generated this correction attribute while the correction attribute which consists of updating data at the time of data modification of this attribute information was generated, and stores in a portable mold storage.
[Claim 6] Said ENI cast address selection processor is an address managerial system according to claim 1 characterized by having the configuration which performs the migration or copy processing of ENI cast

address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.
[Claim 7] Said ENI cast address selection processor is the address managerial system according to claim 1 characterized by to have the configuration which performs the migration or the copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd communication terminal a condition [the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address information by which the electronic signature received from the 1st connected portable mold storage was made].
[Claim 8] Said portable mold storage adds electronic signature to ENI cast address information a condition [authentication formation with a communication terminal], and outputs it to a communication terminal. The communication terminal which received said ENI cast address information and electronic signature It is contingent [on the check of there being no alteration of received data by verification of electronic signature]. The address managerial system according to claim 1 characterized by having the configuration which stores receiving ENI cast address information in the memory in a communication terminal, and is set up as this ENI cast address corresponding to a communication terminal.
[Claim 9] Said ENI cast address selection processor is an address managerial system according to claim 1 characterized by having the configuration which performs data deletion processing from an ENI cast address information management database as recovery processing of this ENI cast address information from a portable mold storage a condition [the check of the ENI cast address information by which electronic signature was made being received, and there being no alteration of the ENI cast address information by verification of this electronic signature].
[Claim 10] The ENI cast address selection processor characterized by having the configuration which outputs the ENI cast address information stored in a portable mold storage a condition [authentication formation with the portable mold storage which is the ENI cast address selection processor which publishes ENI cast address information as the address corresponding to a communication terminal, and serves as an object for address storing].
[Claim 11] The address included in said ENI cast address information is an ENI cast address selection processor according to claim 10 characterized by being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[Claim 12] Said ENI cast address selection processor is an ENI cast address selection processor according to claim 10 characterized by being the configuration which adds and outputs electronic signature to the ENI cast address information stored in a portable mold storage further.
[Claim 13] Said ENI cast address selection processor is an ENI cast address selection processor according to claim 10 characterized by being the configuration which is made to include the attribute information which includes utilization conditions in ENI cast address information, adds the electronic signature for alteration verification to this attribute information, and is outputted to a portable mold storage.
[Claim 14] Said ENI cast address selection processor is an ENI cast address selection processor according to claim 10 characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.
[Claim 15] Said ENI cast address selection processor It is contingent [on the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address information by which the electronic signature received from the 1st connected portable mold storage was made]. The ENI cast address selection processor according to claim 10 characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd portable mold storage.
[Claim 16] Said ENI cast address selection processor is an ENI cast address selection processor according to claim 10 characterized by having the configuration which performs data deletion processing

from an ENI cast address information management database as recovery processing of this ENI cast address information from a portable mold storage a condition [the check of the ENI cast address information by which electronic signature was made being received, and there being no alteration of the ENI cast address information by verification of this electronic signature].
[Claim 17] It is the communication terminal which performs communications processing, and is contingent [on authentication formation with the portable mold storage which equipped this communication terminal with ENI cast address information including the address corresponding to a communication terminal]. It receives from a portable mold storage and is contingent [on the check of there being no alteration of received data by verification of the electronic signature generated to said ENI cast address information]. The communication terminal characterized by having the configuration which stores receiving ENI cast address information in the memory in a communication terminal, and is set up as this ENI cast address corresponding to a communication terminal.
[Claim 18] The address included in said ENI cast address information is a communication terminal according to claim 17 characterized by being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[Claim 19] Information enclosure which is the information enclosure which has the configuration which can be detached and attached freely to a communication terminal, and has a data processing function, and is characterized by having the configuration which stores ENI cast address information including the address corresponding to a communication terminal in memory, reads said ENI cast address information from the memory of information enclosure a condition [authentication formation with this communication terminal], and is outputted to a communication terminal.
[Claim 20] the information enclosure according to claim 19 characterized by having the configuration which performs processing which eliminates said ENI cast address information from the memory of information enclosure while said information enclosure carries out reading appearance of said ENI cast address information from the memory of information enclosure and outputs it to a communication terminal.
[Claim 21] It is the address management method which manages the address set as the communication terminal which performs communications processing, and is contingent [on authentication enactment with an ENI cast address selection processor and a portable mold storage]. The step which outputs ENI cast address information to a portable mold storage from an ENI cast address selection processor, The step at which the portable mold storage which received said ENI cast address information stores receiving ENI cast address information in the memory in a portable mold storage, In the step which outputs ENI cast address information to said communication terminal from a portable mold storage a condition [authentication formation with a portable mold storage and a communication terminal], and said communication terminal The address management method characterized by having the step which sets up the address included in the ENI cast address information which received from said portable mold storage as this ENI cast address corresponding to a communication terminal.
[Claim 22] The address included in said ENI cast address information is an address management method according to claim 21 characterized by being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[Claim 23] Said ENI cast address selection processor Electronic signature is added and outputted to the ENI cast address information stored in a portable mold storage a condition [authentication formation of a portable mold storage]. The portable mold storage which received said ENI cast address information and electronic signature The address management method according to claim 21 characterized by storing receiving ENI cast address information and electronic signature in the memory in a portable mold storage a condition [the check of there being no alteration of received data by verification of electronic signature].
[Claim 24] The address management method according to claim 21 which attribute information including utilization conditions is added and stored in the ENI cast address information stored in a

portable mold storage, and is characterized by being the configuration that the electronic signature for alteration verification was added to this attribute information.
[Claim 25] The address management method according to claim 21 characterized by adding and storing the attribute information which includes utilization conditions in the ENI cast address information stored in a portable mold storage, adding the electronic signature by the device which generated this correction attribute while the correction attribute which consists of updating data at the time of data modification of this attribute information was generated, and storing in a portable mold storage.
[Claim 26] Said ENI cast address selection processor is an address management method according to claim 21 characterized by performing the migration or copy processing of ENI cast address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.
[Claim 27] Said ENI cast address selection processor is an address management method according to claim 21 characterized by to perform the migration or the copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd portable mold storage a condition [the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address information by which the electronic signature received from the 1st connected portable mold storage was made].
[Claim 28] Said portable mold storage adds electronic signature to ENI cast address information a condition [authentication formation with a communication terminal], and outputs it to a communication terminal. The communication terminal which received said ENI cast address information and electronic signature The address management method according to claim 21 characterized by storing receiving ENI cast address information in the memory in a communication terminal a condition [the check of there being no alteration of received data by verification of electronic signature], and setting up as this ENI cast address corresponding to a communication terminal.
[Claim 29] Said ENI cast address selection processor is an address management method according to claim 21 characterized by performing data deletion processing from an ENI cast address information management database as recovery processing of this ENI cast address information from a portable mold storage a condition [the check of the ENI cast address information by which electronic signature was made being received, and there being no alteration of the ENI cast address information by verification of this electronic signature].
[Claim 30] It is the computer program which makes address issuance processing in which the address set as a communication terminal is published perform on computer system. The ENI cast address selection processor which publishes ENI cast address information including the address corresponding to a communication terminal, It is contingent [on authentication formation] to the authentication processing step between the information enclosure which stores the address. In the step which outputs ENI cast address information from an ENI cast address selection processor to information enclosure, and information enclosure The computer program characterized by providing the step which performs electronic signature verification processing to ENI cast address information, and is stored in memory a condition [the check without an alteration].
[Claim 31] The authentication processing step between the storages with which are the computer programs which make the communications processing by utilization of the address set as a communication terminal perform on computer system, and the communication terminal and the communication terminal were equipped, In the step which outputs ENI cast address information to said communication terminal from a storage a condition [authentication formation with a storage and a communication terminal], and said communication terminal The computer program characterized by providing the step which sets up the address included in the ENI cast address information which received from said storage as this ENI cast address corresponding to a communication terminal.

[Translation done.]

JP 2003-051837

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to an address managerial system, an ENI cast address selection processor, a communication terminal, information enclosure and an address management method, and a list at a computer program. Furthermore, it is related with a detail at a computer program at the address managerial system which enabled smooth delivery between the devices of the interface ID in IPv6 (Internet Protocol version 6), an ENI cast address selection processor, a communication terminal, information enclosure and an address management method, and a list.
[0002]
[Description of the Prior Art] In recent years, the personal computer of a pocket mold, a cellular phone, etc. spread, the small communication terminal with which many users have these communication facility and an information processing function is carried, and the communication link which is the outdoors, or connects with a network in a migration place and minds a network is performed.
[0003] In the Internet, IP (Internet Protocol) is used as a communications protocol. IP used now is IPv4, and the address (IP address) which consists of 32 bits as a sending agency / the destination is used. [many] In the Internet communication link, the global IP address which assigns a 32-bit IP address uniquely to each sending agency / destination was adopted, and each sending agency / destination are distinguished according to an IP address. However, the world of the Internet shows breadth quickly and an exhaustion of the address space where IPv4 was restricted, i.e., a global address, is posing a problem. In order to solve this, in IETF (Internet EngineeringTask Force), new IPv6 (Internet Protocol version 6) which extends IP address space to 128 bits from 32 bits as a next-generation IP address is proposed.
[0004] IPv6 is the present succeeding protocol of IPv4, and has the address format shown in drawing 1 . IPv6 is 128 bit patterns, it is the interface ID as a node identifier for a lower bit to identify a node uniquely on the Internet or a subnet (Interface ID) (for example, IEEE802 format), and a high order bit is a network prefix (Network Prefix) as a location specifier which shows the subnetwork which the node has connected. Therefore, the terminal unit which belongs to the same subnetwork fundamentally becomes what has the same network prefix (Network Prefix) which the high order bit of the IPv6 address shows.
[0005] In IPv6, since delivery of a packet is performed only based on a prefix and a subnet number, in a device manufacture manufacturer, assignment of the low-ranking address ID, i.e., an interface, is attained from it. A part of interface ID number is a manufacture manufacturer identifier, and the part which remained is left to discretion of a manufacturer at accuracy. Therefore, unlike IPv4, by IPv6, a manufacturer can determine freely some of interfaces ID, i.e., IPv6 address, and it becomes possible to connect customer information with matching it with user ID to the device put on the market through Interface ID.
[0006] However, actually, a response with Interface ID and a customer is not fixed, and is changed. This

originates in customer action of a change of the terminal by the user etc. Response-related fluctuation of such an Interface ID and a customer has an adverse effect on the application which matches and uses a user and an IP address like IP telephone. For example, in the case of IP telephone, the data in which a telephone partner's generic name is shown, and associated data with the IP address of a actual communications-partner device are held as an address solution device, and offering service based on this associated data is performed.

[0007] However, the communication link by the bought device cannot be performed until correction processing of associated data is completed, when the response relation between Interface ID and a user changes by customer action of the terminal change by the user etc. Although packet delivery is due to a prefix and a subnet number, it is because it determines whether an IPv6 device compare the whole IPv6 address including Interface ID at the last of delivery, and receive a packet.

[0008] As for such a situation, it is desirable to be avoided for the application as which very strong availability is required like a telephone. In the conventional configuration, it was thought that it was difficult to apply IPv6 in which the response relation between Interface ID and a customer may collapse to the application of which high availability is required like a cellular phone.

[0009]

[Problem(s) to be Solved by the Invention] This invention is conventionally made in view of the above-mentioned trouble in a configuration, is treating the ENI cast device of IPv6 as ID of a user proper, makes the environment where the service according to user individual can be offered, and provides with a computer program the address managerial system which raises convenience, an ENI cast address selection processor, a communication terminal, information enclosure and an address management method, and a list.

[0010] The address of IPv6 defines three kinds of addresses, a unicast, the ENI cast, and a multicast. A unicast is an identifier which directs a single interface and a packet is delivered by the single interface which a unicast address shows. The ENI cast is an identifier which points out the set of two or more interfaces, and a packet is delivered from the interface which the address shows by one nearest interface chosen based on the range measurement by the path control protocol. A multicast is an identifier which points out the set of two or more interfaces, and a packet is delivered by all the interfaces that the address shows.

[0011] It is like [the ENI cast is the model with which a service request is advanced to two or more terminals, and one or more of them give their service, and] the so-called representation call service. The IPv6 version of the primary directory number at this time is the ENI cast address.

[0012] The address common to all devices can be assigned by treating the ENI cast address as a thing of a user proper, and in case it is modification of a device, it becomes unnecessary to change the address. Since a simultaneously realizable advantage also has ENI cast mold service, this technique is promising.

[0013] It aims at providing with a computer program the address managerial system which can perform troublesome ID setting out easily, an ENI cast address selection processor, a communication terminal, information enclosure and an address management method, and a list in this invention, preventing unjust ID activity by using the portable mold storage which has a digital contents protection feature.

[0014]

[Means for Solving the Problem] The communication terminal which the 1st side face of this invention is an address managerial system which manages the address set as the communication terminal which performs communications processing, and serves as an address selection object, The portable mold storage which equips said communication terminal and stores the ENI cast address, It has the ENI cast address selection processor which publishes ENI cast address information as the address corresponding to this communication terminal, and said ENI cast address selection processor is subject [to authentication formation of a portable mold storage]. The portable mold storage which outputted ENI cast address information to said portable mold storage, and received said ENI cast address information Receiving ENI cast address information is stored in the memory in a portable mold storage, and it is

contingent [on authentication formation with the connected communication terminal]. ENI cast address information is outputted to said communication terminal. Said communication terminal It is in the address managerial system characterized by having the configuration which sets up the address included in the ENI cast address information which received from said portable mold storage as this ENI cast address corresponding to a communication terminal.

[0015] Furthermore, in one embodiment of the address managerial system of this invention, it is characterized by the address included in said ENI cast address information being the interface ID which constitutes the lower bit in the address structure specified in IPv6.

[0016] In one embodiment of the address managerial system of this invention furthermore, said ENI cast address selection processor Electronic signature is added and outputted to the ENI cast address information stored in a portable mold storage a condition [authentication formation of a portable mold storage]. The portable mold storage which received said ENI cast address information and electronic signature It is characterized by storing receiving ENI cast address information and electronic signature in the memory in a portable mold storage a condition [the check of there being no alteration of received data by verification of electronic signature].

[0017] Furthermore, in one embodiment of the address managerial system of this invention, attribute information including utilization conditions is added and stored in the ENI cast address information stored in a portable mold storage, and it is characterized by being the configuration that the electronic signature for alteration verification was added to this attribute information.

[0018] Furthermore, it is characterized by to be the configuration which the attribute information which includes utilization conditions in the ENI cast address information stored in a portable mold storage is added and stored, adds the electronic signature by the device which generated this correction attribute while the correction attribute which consists of updating data at the time of data modification of this attribute information was generated in one embodiment of the address managerial system of this invention, and stores in a portable mold storage.

[0019] Furthermore, in one embodiment of the address managerial system of this invention, said ENI cast address selection processor is characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.

[0020] In one embodiment of the address managerial system of this invention furthermore, said ENI cast address selection processor It is contingent [on the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address information by which the electronic signature received from the 1st connected portable mold storage was made]. It is characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd communication terminal.

[0021] In one embodiment of the address managerial system of this invention furthermore, said portable mold storage Add electronic signature to ENI cast address information a condition [authentication formation with a communication terminal], and it outputs to a communication terminal. The communication terminal which received said ENI cast address information and electronic signature It is characterized by having the configuration which stores receiving ENI cast address information in the memory in a communication terminal a condition [the check of there being no alteration of received data by verification of electronic signature], and is set up as this ENI cast address corresponding to a communication terminal.

[0022] In one embodiment of the address managerial system of this invention furthermore, said ENI cast address selection processor The ENI cast address information by which electronic signature was made from the portable mold storage is received, and it is contingent [on the check of there being no alteration of the ENI cast address information by verification of this electronic signature]. It is characterized by having the configuration which performs data deletion processing from an ENI cast address information

management database as recovery processing of this ENI cast address information.
[0023] Furthermore, the 2nd side face of this invention is in the ENI cast address selection processor characterized by having the configuration which outputs the ENI cast address information stored in a portable mold storage a condition [authentication formation with the portable mold storage which is the ENI cast address selection processor which publishes ENI cast address information as the address corresponding to a communication terminal, and serves as an object for address storing].
[0024] Furthermore, in one embodiment of the ENI cast address selection processor of this invention, it is characterized by the address included in said ENI cast address information being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[0025] Furthermore, in one embodiment of the ENI cast address selection processor of this invention, said ENI cast address selection processor is characterized by being the configuration which adds and outputs electronic signature to the ENI cast address information stored in a portable mold storage further.

[0026] Furthermore, in one embodiment of the ENI cast address selection processor of this invention, said ENI cast address selection processor is characterized by being the configuration which is made to include the attribute information which includes utilization conditions in ENI cast address information, adds the electronic signature for alteration verification to this attribute information, and is outputted to a portable mold storage.
[0027] Furthermore, in one embodiment of the ENI cast address selection processor of this invention, said ENI cast address selection processor is characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.
[0028] In one embodiment of the ENI cast address selection processor of this invention furthermore, said ENI cast address selection processor It is contingent [on the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address information by which the electronic signature received from the 1st connected portable mold storage was made]. It is characterized by having the configuration which performs the migration or copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd portable mold storage.
[0029] In one embodiment of the ENI cast address selection processor of this invention furthermore, said ENI cast address selection processor The ENI cast address information by which electronic signature was made from the portable mold storage is received, and it is contingent [on the check of there being no alteration of the ENI cast address information by verification of this electronic signature]. It is characterized by having the configuration which performs data deletion processing from an ENI cast address information management database as recovery processing of this ENI cast address information.
[0030] Furthermore, the 3rd side face of this invention is a communication terminal which performs communications processing, and it is contingent [on authentication formation with the portable mold storage which equipped this communication terminal with ENI cast address information including the address corresponding to a communication terminal]. It receives from a portable mold storage and is contingent [on the check of there being no alteration of received data by verification of the electronic signature generated to said ENI cast address information]. It is in the communication terminal characterized by having the configuration which stores receiving ENI cast address information in the memory in a communication terminal, and is set up as this ENI cast address corresponding to a communication terminal.
[0031] Furthermore, in one embodiment of the communication terminal of this invention, it is characterized by the address included in said ENI cast address information being the interface ID which constitutes the lower bit in the address structure specified in IPv6.
[0032] Furthermore, the 4th side face of this invention is in the information enclosure which is the information enclosure which has the configuration which can be detached and attached freely to a

communication terminal, and has a data processing function, and is characterized by to have the configuration which stores ENI cast address information including the address corresponding to a communication terminal in memory, reads said ENI cast address information from the memory of information enclosure a condition [authentication formation with this communication terminal], and is outputted to a communication terminal.

[0033] Furthermore, in one embodiment of the information enclosure of this invention, said information enclosure is characterized by having the configuration which performs processing which eliminates said ENI cast address information from the memory of information enclosure while it reads said ENI cast address information from the memory of information enclosure and outputs it to a communication terminal.

[0034] Furthermore, the 5th side face of this invention is an address management method which manages the address set as the communication terminal which performs communications processing, and is subject [to authentication enactment with an ENI cast address selection processor and a portable mold storage]. The step which outputs ENI cast address information to a portable mold storage from an ENI cast address selection processor, The step at which the portable mold storage which received said ENI cast address information stores receiving ENI cast address information in the memory in a portable mold storage, In the step which outputs ENI cast address information to said communication terminal from a portable mold storage a condition [authentication formation with a portable mold storage and a communication terminal], and said communication terminal It is in the address management method characterized by having the step which sets up the address included in the ENI cast address information which received from said portable mold storage as this ENI cast address corresponding to a communication terminal.

[0035] Furthermore, in one embodiment of the address management method of this invention, it is characterized by the address included in said ENI cast address information being the interface ID which constitutes the lower bit in the address structure specified in IPv6.

[0036] In one embodiment of the address management method of this invention furthermore, said ENI cast address selection processor Electronic signature is added and outputted to the ENI cast address information stored in a portable mold storage a condition [authentication formation of a portable mold storage]. The portable mold storage which received said ENI cast address information and electronic signature It is characterized by storing receiving ENI cast address information and electronic signature in the memory in a portable mold storage a condition [the check of there being no alteration of received data by verification of electronic signature].

[0037] Furthermore, in one embodiment of the address management method of this invention, attribute information including utilization conditions is added and stored in the ENI cast address information stored in a portable mold storage, and it is characterized by being the configuration that the electronic signature for alteration verification was added to this attribute information.

[0038] Furthermore, it is characterized by to add and store the attribute information which includes utilization conditions in the ENI cast address information stored in a portable mold storage, to add the electronic signature by the device which generated this correction attribute while the correction attribute which consists of updating data at the time of data modification of this attribute information was generated in one embodiment of the address management method of this invention, and to store in a portable mold storage.

[0039] Furthermore, in one embodiment of the address management method of this invention, said ENI cast address selection processor is characterized by performing the migration or copy processing of ENI cast address information which outputs the ENI cast address information received from the 1st connected portable mold storage to other 2nd portable mold storage.

[0040] In one embodiment of the address management method of this invention furthermore, said ENI cast address selection processor It is contingent [on the check of there being no alteration of the ENI cast address information by verification of the electronic signature about the ENI cast address

information by which the electronic signature received from the 1st connected portable mold storage was made]. It is characterized by performing the migration or copy processing of ENI cast address information which outputs this ENI cast address information to other 2nd portable mold storage.
[0041] In one embodiment of the address management method of this invention furthermore, said portable mold storage Add electronic signature to ENI cast address information a condition [authentication formation with a communication terminal], and it outputs to a communication terminal. The communication terminal which received said ENI cast address information and electronic signature It is characterized by storing receiving ENI cast address information in the memory in a communication terminal a condition [the check of there being no alteration of received data by verification of electronic signature], and setting up as this ENI cast address corresponding to a communication terminal.
[0042] Furthermore, in one embodiment of the address management method of this invention, said ENI cast address selection processor receives the ENI cast address information by which electronic signature was made from the portable mold storage, and is characterized by performing data deletion processing from an ENI cast address information management database as recovery processing of this ENI cast address information a condition [the check of there being no alteration of the ENI cast address information by verification of this electronic signature].
[0043] Furthermore, the 6th side face of this invention is a computer program which makes address issuance processing in which the address set as a communication terminal is published perform on computer system. The ENI cast address selection processor which publishes ENI cast address information including the address corresponding to a communication terminal, It is contingent [on authentication formation] to the authentication processing step between the information enclosure which stores the address. In the step which outputs ENI cast address information from an ENI cast address selection processor to information enclosure, and information enclosure Electronic signature verification processing to ENI cast address information is performed, and it is in the computer program characterized by providing the step stored in memory a condition [the check without an alteration].
[0044] Furthermore, the 7th side face of this invention is a computer program which makes the communications processing by utilization of the address set as a communication terminal perform on computer system. The authentication processing step between the storages with which the communication terminal and the communication terminal were equipped, In the step which outputs ENI cast address information to said communication terminal from a storage a condition [authentication formation with a storage and a communication terminal], and said communication terminal It is in the computer program characterized by providing the step which sets up the address included in the ENI cast address information which received from said storage as this ENI cast address corresponding to a communication terminal.
[0045] In addition, the computer program of this invention is a computer program which can be offered to the general purpose computer system which can perform various program codes, for example by communication media, such as record media, such as a storage offered in a computer-readable format, communication media, for example, CD, and FD, MO, or a network. By offering such a program in a computer-readable format, processing according to a program is realized on computer system.
[0046] The object, the description, and advantage of further others of this invention will become [rather than] clear by detailed explanation based on the example and the drawing to attach of this invention mentioned later. In addition, in this description, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.
[0047]
[Embodiment of the Invention] Hereafter, the address managerial system of this invention, an ENI cast address selection processor, a communication terminal, information enclosure, and an address management method are explained to a detail, referring to a drawing.
[0048] The outline of the address managerial system of this invention is explained using drawing 2 . In the address managerial system of this invention, the device which performs data communication using

the address (IPv6 address) is the user terminal 130 as a communication terminal which has communication facility, and this is devices, such as a cellular phone and PDA. The application utilization processing which matched the user and the IP address like for example, IP telephone is possible for these user terminals.

[0049] A user terminal 130 has a removable configuration for the portable mold storage 120 which carried the flash memory. In addition, the portable mold storage 120 is information enclosure which has CPU and performs information storing to memory, elimination, and read-out to the bottom of control of CPU and for which information can be processed. By performing data transfer between the ENI cast address selection processor 110 and the portable mold storage 120, reception storing of the interface ID which is the low order bit address of the IPv6 ENI cast address is carried out from the ENI cast address selection processor 110 at the portable mold storage 120. A user terminal 130 is equipping with the portable mold storage 120 which stored the ENI cast address (interface ID), and uses the ENI cast address (interface ID) stored in the portable mold storage 120 as the address of a user terminal 130.

[0050] In addition, it is premised on using the interface ID of the IPv6 address for an ENI cast application in this example. Hereafter, Interface ID shall be pointed out in the language ENI cast "address." Since the ENI cast address of a definition of IPv6 original points out the whole IPv6 address which added the subnet number and the prefix to Interface ID, it differs from the ENI cast address said here. If the ENI cast address said here is expressed more to accuracy, it becomes the interface ID prepared for the ENI cast application. The interface ID stored in the portable mold storage 120 is the interface ID prepared for the ENI cast application.

[0051] The ENI cast address selection processor 110 communicates with the portable mold storage 120, and transmits the available ENI cast address of a user terminal 130 to the portable mold storage 120. The portable mold storage 120 receives the ENI cast address, and stores it in memory.

[0052] The ENI cast address selection processor 110 has an ENIKYATOSUTO address-generation means 111 to generate the new ENI cast address according to the demand from the outside. The digital contents safeguard 112 detects the inaccurate ENI cast address, an unjust address alteration, etc. It also has the function to correct it depending on the case. The digital contents safeguard 112 performs processing of the check of the information about authentication [of the devices in the ENI cast information transfer processing between the portable mold storages 120], electronic signature verification [as inspection about the justification of ENI cast information], check [of the count limit of a copy], and issuance origin etc.

[0053] The ENI cast address selection processor 110 has the ENI cast address administration database 113 in the interior or the exterior, and it performs issuance processing of the ENI cast address to the connected portable mold storage 120, managing so that issuance of the ENI cast address which overlapped the generate time of the ENI cast address in the ENIKYATOSUTO address-generation means 111 with reference to the ENI cast address administration database 113 may not be made.

[0054] The ENI cast address selection processor 110 performs recovery of the ENI cast address from the portable mold storage 120, or processing which eliminates the ENI cast address of the portable mold storage 120 interior other than the issuance processing of the ENI cast address to the portable mold storage 120. Furthermore, the registration of the ENI cast address administration database 113 based on the ENI cast address accepted the need and eliminated [published, collected and] and an update process are performed.

[0055] The portable mold storage 120 has the ENI cast address storing means 121 constituted by the flash memory. The available ENI cast address and the information about it are stored in the ENI cast address storing means 121 by the user terminal 130. For example, information, such as a purchaser of the ENI cast address, an expiration date, a count of a copy, and electronic signature, is stored. The number of the ENI cast addresses written in the portable mold storage 120 can be considered as plurality. The information (for example, service interface which the owner name of the address, the key value for authentication, and its address receive) relevant to the ENI cast address can also be held combining the

address.
[0056] The digital contents safeguard 122 in the portable mold storage 120 Authentication of the devices in the ENI cast information transfer processing between the ENI cast address selection processors 110, and the electronic signature verification as inspection about the justification of ENI cast information, Processing of the check of the information about check [of the count limit of a copy] and issuance origin etc. is performed. Furthermore, processing of the check of the information about authentication [of the devices in the ENI cast information reading processing from a user terminal 130], electronic signature verification [as inspection about the justification of ENI cast information], check [of the count limit of a copy], and issuance origin etc. is performed. A user terminal 130 has a removable configuration for the portable mold storage 120 which carried the flash memory. It is a device corresponding to IPv6 which recognizes the ENI cast address stored in the memory of the portable mold storage 120, and is used as the setting-out address of self by equipping with the portable mold storage 120. The activity as a usual IPv6 device is also possible, and it has the interface ID corresponding to IPv6 of a device proper.
[0057] The ENI cast address utilization application executive operation means 131 in a user terminal 130 is an application program executive operation means as a means to perform application utilization processing which matched the user and the IP address like for example, IP telephone, and a means to perform TV phone service using the ENI cast address.
[0058] The digital contents safeguard 132 in a user terminal 130 performs processing of the check of the information about authentication [of the devices in the ENI cast information transfer processing between the portable mold storages 120 which stored the ENI cast address], electronic signature verification [as inspection about the justification of ENI cast information], check [of the count limit of a copy], and issuance origin etc.
[0059] Next, the example of a hardware configuration of a user terminal, a portable mold storage, and an ENI cast address selection processor is explained using drawing 3 . First, the configuration of a user terminal 310 is explained. CPU (Central processing Unit)311 performs various operation and an application program. Specifically, control of processing of the input/output operation of human being who operates upper layer protocol processing and the terminal of IPv6, and the ENI cast address transceiver processing performed between portable mold storages, authentication processing, etc. are performed. ROM (Read-Only-Memory)312 stores the fixed data as the program which CPU311 performs, or an operation parameter. RAM (Random Access Memory)313 is used as the storage area of the program performed in processing of CPU311, and the parameter which changes suitably in program manipulation, and a work-piece field.
[0060] The input section 314 is operated by the user in order to input various kinds of commands into CPU311. The output section 315 is LCD (liquid crystal display) etc., and displays various information by the text or the image.
[0061] The interface (I/F) 316 corresponding to IPv6 offers the channel which can communicate using an IPv6 protocol. It communicates with the router of a connection subnet etc., and packet-ize the data supplied from CPU311 and the RAM315 grade, and it transmits, or processing which receives a packet through a router is performed. RTC317 is not used when preparing the expiration date in ENI cast address information, and it is not indispensable. RTC measures IPv6 communication link time amount. It is used in order to subtract measurement time amount from the available time which accompanies the ENI cast address then used and to update ENI cast address information in the form of a correction attribute (after-mentioned).
[0062] It realizes as nonvolatile memory which stores the interface ID corresponding to IPv6 set as the user terminal, and the interface ID storing memory 318 corresponding to IPv6 is not eliminated also after the power source of a user terminal has fallen. R/W of data is controlled by CPU311. The communication link socket 319 is a communications interface with a portable mold storage.
[0063] Next, the configuration of the portable mold storage 320 is explained. CPU (Central processing

Unit)321 performs various operation and an application program. Specifically, control of the ENI cast address transceiver processing performed between the data storage read-out control to the memory of a portable mold storage, data encryption, decode processing, signature generation, verification processing, a user terminal, or an ENI cast address selection processor, authentication processing, etc. are performed. ROM (Read-Only-Memory)322 stores the fixed data as the program which CPU311 performs, or an operation parameter. RAM (Random Access Memory)323 is used as the storage area of the program performed in processing of CPU321, and the parameter which changes suitably in program manipulation, and a work-piece field.

[0064] Interface ID storing memory 324 is realized as nonvolatile memory which stores the ENI cast address (interface ID) corresponding to IPv6 which received from the ENI cast address selection processor. Storing of data, read-out, and elimination are performed by control of CPU (Central processing Unit)321.

[0065] A communication plug 325 is an interface which sets up the channel used in case the communication link with a user terminal is performed, it connects with those with an interface which make read-out of the ENI cast address possible, and the ENI cast address selection processor 330 and new issue processing of the ENI cast address, recovery processing, and elimination processing are performed.

[0066] Next, the configuration of the ENI cast address selection processor 330 is explained. CPU (Central processing Unit)331 performs various operation and an application program. Specifically, control of the ENI cast address transceiver processing performed between the portable mold storages 320, authentication processing, etc. are performed. ROM (Read-Only-Memory)332 stores the fixed data as the program which CPU331 performs, or an operation parameter. RAM (Random Access Memory)333 is used as the storage area of the program performed in processing of CPU331, and the parameter which changes suitably in program manipulation, and a work-piece field.

[0067] The input section 334 is operated by the user in order to input various kinds of commands into CPU331. The output sections 335 are CRT, LCD (liquid crystal display), etc., and display various information by the text or the image.

[0068] The ENI cast address administration database 336 is a database for issuance management of the ENI cast address, and stores a user, a device and the matching data of the ENI cast address, expiration date management data, etc. In addition, although this example shows the example which constituted the ENI cast address administration database 336 in the ENI cast address selection processor 330 interior, it is good also as a configuration which constitutes a database as a network connection external database, and is shared between two or more ENI cast address selection processors.

[0069] The communication link socket 337 is an interface which sets up the channel used in case it connects with the portable mold storage 320 and new issue processing of the ENI cast address, recovery processing, and elimination processing are performed.

[0070] Next, the outline of the concrete example of processing in the address managerial system of this invention is explained using drawing 4 . It explains as an example in which the firm which he is here should do the item sale of the ENI cast address, and entrusted the sale to the dealer. In addition, as explained previously, the device using the address (IPv6 address) is a user terminal, and this is devices, such as a cellular phone and PDA. A user terminal equips with the portable mold storage which stored the ENI cast address, and performs the communication link which used the ENI cast address stored in the portable mold storage as the ENI cast address (interface ID) of self. Storing of the ENI cast address, recovery, and elimination are performed by connecting a portable mold storage to an ENI cast address selection processor.

[0071] A user terminal and a portable mold storage have a digital contents safeguard, as mentioned above, respectively, and the data applied to the authentication processing in the case of communications processing with other devices and cipher processing, for example, cryptographic key data, are written in ROM, and they are shipped.

[0072] In a dealer, by considering the ENI cast address as an item sale, after performing ENI cast address write-in setting-out processing to a portable mold storage, it provides for a user. Or ENI cast address write-in setting-out processing is performed to the portable mold storage which the user carried in. An ENI cast address selection processor performs this processing, as drawing 2 or drawing 3 explained, the portable mold storage and ENI cast address selection processor which are set as the storing object of the ENI cast address are connected, and ENI cast address storing processing is performed a condition [formation of authentication processing].
[0073] In a dealer, recovery processing of the ENI cast address [finishing / not only new ENI cast address issuance processing but storing in a portable mold storage] and elimination processing of the ENI cast address [still finishing / storing in a portable mold storage] are performed.
[0074] A dealer holds an ENI cast address selection processor, when a customer purchases the ENI cast address, it uses an ENI cast address selection processor, and it writes the ENI cast address in a customer's portable mold storage. At this time, the various information about a customer is registered into an ENI cast address selection processor and a portable mold storage at coincidence combining the ENI cast address which made a new issue. It is the device which has digital contents protection features, such as a memory stick, as a portable mold storage.
[0075] The content of the ENI cast address information registered into an ENI cast address selection processor and a portable mold storage is shown in drawing 5 . The left-hand side of drawing 5 shows the situation of the ENI cast address information stored in the portable mold storage (S), and it is shown that two or more ENI cast address information is storable in one portable mold storage (S). The right-hand side of drawing showed one ENI cast address information of them to the detail. ENI cast information has digital signature SA1 which the configurator of digital signature SO which the IPv6 ENI cast address AA and its generation person give also at the lowest, the initial attribute AT 1, and an attribute gives. In the example of drawing, although two, the number which can be copied, and available time, are shown as an attribute, the class and number of attributes can be changed suitably and the configurator of an attribute stores required information.
[0076] A copy available number is a copy limit count which shows that copy authorization upper limit which may carry out a division copy and may save the IPv6 ENI cast address AA at how many portable mold storages. Available time is the die length of the time amount which can use the IPv6 ENI cast address AA. According to the IPv6 communication link time amount measured by RTC constituted by the user terminal, from the available time, measurement time amount is subtracted and this information is updated.
[0077] In case information is rewritten by the copy of the IPv6 ENI cast address AA, and utilization, updating data are added to ENI cast address information in the correction attributes AT2 and AT3 and the form of ... These correction attributes are added to ENI cast address information with the digital signature which the device which performed each correction, i.e., a user terminal, a portable mold storage, or an ENI cast address selection processor generates. ENI cast address information is exchanged between an ENI cast address selection processor, a portable mold storage, and each user terminal, and an information addressee inspects the existence of an alteration by signature verification each time.
[0078] A customer (user) can distribute the purchased ENI cast address to the various devices as various communication terminals which a user owns by copying to two or more portable mold storages, and can share the ENI cast address among them. As a result, ENI cast service is shared among those devices. For example, by equipping with the memory stick which has the same ENI cast address in the AV equipment which has a memory stick terminal, ENI cast service can be offered among them. Devices, such as PC which a user owns as a device used for a copy activity, a cellular phone, and PDA, can be used.
[0079] Moreover, a user has the unnecessary ENI cast address then [drag-in and], the portable mold storage which wrote in the ENI cast address which became unnecessary eliminated from a portable mold storage in a dealer using an ENI cast address selection processor, when the ENI cast address becomes unnecessary. At this time, the response relation between the ENI cast address, customer information, and

others is simultaneously eliminated from a portable mold storage and an ENI cast address selection processor.

[0080] Issuance processing of the ENI cast address of as opposed to [processing / which is hereafter performed in the system of this invention] the portable mold storage from (1) ENI cast address selection processor, (2) Minded the migration processing (3) ENI cast address selection processor of the ENI cast address through an ENI cast address selection processor between different portable mold storages. The detail of each processing is explained beyond utilization processing (5) ENI cast address return (recovery) processing of the copy processing (4) ENI cast address of the ENI cast address between different portable mold storages.

[0081] [issuance processing of the ENI cast address to the portable mold storage from (1) ENI cast address selection processor] -- the detail of the issuance processing of the ENI cast address to a portable mold storage is first explained from an ENI cast address selection processor. Drawing which explains the processing sequence in ENI cast address new issue processing to drawing 6 is shown. A portable mold storage here is a portable mold storage which is not used yet after shipment from works, and the ENI cast address is not written in the memory of a portable mold storage.

[0082] First, a communication plug mutual [between ENI cast address selection processors] and a communication link socket are connected with a portable mold storage. Authentication processing will be performed if connection is made. Authentication processing is performed as check processing of both the devices that perform a communication link being just devices. the approach of combining a public key authentication method, a common key authentication method, Kerberos that has a track record by IPv4, and digital watermarking as authentication processing -- or the approach of designing and mounting interface specification which SDMI (Secure Digital Music Initiative) advocates etc. is employable.

[0083] The processing sequence of a public key authentication method is explained using drawing 7 as an example of authentication processing. For activation of a public key cryptosystem, public key Kpub-Sn of a portable mold storage (Sn), private key Kpri-Sn, and the public key certificate CertSn are stored in ROM of a portable mold storage as authentication data, and, on the other hand, public key Kpub-W, private key Kpri-W, and the public key certificate CertW are stored in the ENI cast address selection processor (W).

[0084] In drawing 7 , first, an ENI cast address selection processor generates a random number Rb, and is sent to a portable mold storage. It calculates Va by a portable mold storage generating random numbers Ra and Ka, and carrying out the multiplication of G and Ka which are a point (base point) common to a system on the elliptic curve E applied in a public key cryptosystem. With the electronic signature furthermore performed to data Ra||Rb||Va using its own private key (KPri-Sn), data (CertSn||Ra||Rb||Va) besides a public key certificate (CertSn) are sent to an ENI cast address selection processor. Electronic signature uses a general digital signature technique, for example, RSA cryptograph, the message digest method realized combining Hash Function SHA-1.

[0085] An ENI cast address selection processor inspects the justification of the public key certificate (CertSn) of a portable mold storage, and the justification of a signature. When justification is checked, an ENI cast address selection processor generates a random number Kb, and sends the signature data given to data Rb||Ra||Vb using their own private key (KPri-W) with data (CertW||Rb||Ra||Vb) besides a public key certificate to a portable mold storage.

[0086] Then, in a portable mold storage, the justification of the public key certificate (CertW) of an ENI cast address selection processor and the justification of a signature are inspected. When justification is checked, with an ENI cast address selection processor, the multiplication of Kb and the Va is carried out for Ka and Vb on an elliptic curve E, respectively, and the session key Ks is obtained. The session key Ks as a cryptographic key which mutual recognition is made with an ENI cast address selection processor and a portable mold storage by the above technique, and is applied by subsequent data communication by it is sharable.

[0087] Explanation is continued about return and an ENI cast address new issue processing sequence to drawing 6 . When it is checked that mutual is a just device, in mutual recognition processing which was explained by drawing 7 next, an ENI cast address selection processor As opposed to the ENI cast address information (A.I. Artificial Intelligence) which performed and generated ENI cast address information (A.I. Artificial Intelligence) generation processing Electronic signature is performed by private key Kpri-W of self, and further, it enciphers by public key Kpub-Sn of the portable mold storage acquired on the occasion of previous authentication processing, and transmits to a portable mold storage. In addition, although this example explains the example which applied a partner's public key as a key for encryption processing in the data communication between mutual devices, it is good also as a configuration which performs a communication link data encryption using the session key shared at the time of the mutual recognition in a public key cryptosystem.

[0088] After the portable mold storage which received the enciphered ENI cast address information performs decode processing for received data by private key Kpri-Sn of self, it performs verification of electronic signature to ENI cast address information with the application of public key Kpub-W of an ENI cast address selection processor, and judges the existence of an alteration. In addition, although electronic signature is explained as an example currently made with the private key of an ENI cast address selection processor, it is good also as a configuration with which the signature is made with other ID issuance engines' private key, and stores the public key of ID issuance engine for signature verification in the portable mold storage which performs signature verification in this case here.

[0089] If it judges with a portable mold storage not having an alteration in ENI cast address information by signature verification, ENI cast address information including electronic signature is stored in the interface ID storing memory 324 at the basis of control of CPU320 shown in drawing 3 . A portable mold storage transmits a confirmation-of-receipt response to an ENI cast address selection processor after these processings. An ENI cast address selection processor receives a confirmation-of-receipt response, and processing is completed.

[0090] Migration processing of the ENI cast address through [migration processing of the ENI cast address through (2) ENI cast address selection processor between different portable mold storages], next an ENI cast address selection processor between different portable mold storages is explained with reference to drawing 8 .

[0091] In migration processing of the ENI cast address between different portable mold storages, the address output former portable mold storage 801 which suspends the activity of the ENI cast address and outputs the address, and the address output point portable mold storage 802 which stores the ENI cast address newly and starts an activity are connected to an ENI cast address selection processor one by one, and processing is performed.

[0092] The ENI cast address information to which electronic signature was added is written in the memory (interface ID storing memory 324 in drawing 3) of the address output former portable mold storage 801.

[0093] First, between ENI cast address selection processors is connected with the address output former portable mold storage 801 which suspends the activity of the ENI cast address and outputs the address, and mutual recognition processing is performed. the approach of combining a public key authentication method, a common key authentication method, Kerberos that has a track record by IPv4, and digital watermarking as authentication processing, as mentioned above -- or the approach of designing and mounting interface specification which SDMI (Secure DigitalMusic Initiative) advocates etc. is employable.

[0094] When it is checked that mutual is a just device, in mutual recognition processing next, the address output former portable mold storage 801 The ENI cast address information written in the memory in an address output former portable mold storage is read. Generate the signature by the self private key and encryption processing of transmit data is further performed using the public key of the ENI cast address selection processor which is a session key or a communications partner. It transmits to

an ENI cast address selection processor as encryption ENI cast address information with a signature.
[0095] If the ENI cast address information enciphered from the address output former portable mold storage 801 is received, an ENI cast address selection processor performs decode processing with the application of a session key or a self private key, further, will perform signature verification with the application of the public key of an address output former portable mold storage, and will check the existence of a data alteration. Furthermore, attribute verification processing is performed.
[0096] The procedure of signature verification and attribute verification processing is explained using drawing 9 . First, the data addressee who performs signature verification and attribute verification processing will verify electronic signature about the ENI cast address (drawing 5 , AA) in step S101, if ENI cast address information is received. A verification person shall acquire beforehand the public key of the generation person of the ENI cast address. In S102, if it becomes an error by verification of a signature, the ENI cast address AA is judged to be what was altered, will perform a certain processing to the ENI cast address at step S111, and will forbid an activity. For example, the elimination command of the address is transmitted to a portable mold storage, and elimination processing is performed.
[0097] In verification of the electronic signature about the ENI cast address AA in step S101, when judged with having no data alteration (it is Yes at S102), it progresses to step S103 and the justification of electronic signature is investigated about an initial attribute (drawing 5 , AT1). As for the point and a verification person, this also acquires an attribute grant person's public key. The public keys applied to certification verification here may differ, when the same as the issuer of ENI cast address information. In S104, if it becomes an error by verification of a signature, the initial attribute AT 1 is judged to be what was altered, will perform a certain processing to the ENI cast address at step S111, and will forbid an activity. It eliminates in this example of implementation.
[0098] Next, in step S105, it investigates whether the correction attribute which should be verified further exists. As mentioned above, when renewal of an attribute is needed with the copy of the ENI cast address AA, and utilization, updating data are added to ENI cast address information in the correction attributes AT2 and AT3 and the form of ... These correction attributes are added to ENI cast address information with the digital signature which the device which performed each correction, i.e., a user terminal, a portable mold storage, or an ENI cast address selection processor generates. The existence of such a correction attribute is judged at step S105. When there is no correction attribute, it ends, and in step S110, all signature verification judges with ENI cast address information being just, and ends processing.
[0099] When there is a correction attribute, it progresses to step S106 and signature verification of a correction attribute which is not verifying is performed. Attribute value is read to the old order (added order) of correction, and a series of inspection is conducted. the content of inspection comes out of whether the correction whose 3 available time increases [whether the correction to which one signature of a count / the right, or / (S107) and the count of 2 copies / increases exists, and] (S108) exists (S109). Another check is performed, although the check mentioned above is performed in this example of implementation in order [the count of a copy and whose available time decrease] to use and to realize only the direction. These inspection is conducted in order of correction to all correction attributes. If it succeeds in all the above inspection, inspection will be completed, but when one or more inspection goes wrong, in S111, a certain processing is performed to the ENI cast address information, and an activity is forbidden. It eliminates in this example of implementation.
[0100] Explanation is continued to drawing 8 about the sequence of migration processing of the ENI cast address between return and a different portable mold storage. An ENI cast address selection processor will transmit a confirmation-of-receipt response to the address output former portable mold storage 801 by it, if the justification of data is checked by signature verification of the ENI cast address information which received from the address output former portable mold storage 801 etc., and the address output former portable mold storage 801 performs elimination processing of the ENI cast address based on an Acknowledgement.

[0101] Next, in an ENI cast address selection processor, the address output point portable mold storage 802 is connected. Authentication processing will be performed if connection is made. Authentication processing is performed as check processing of both the devices that perform a communication link being just devices. the approach of combining a public key authentication method, a common key authentication method, Kerberos that has a track record by IPv4, and digital watermarking as authentication processing -- or the approach of designing and mounting interface specification which SDMI (Secure Digital Music Initiative) advocates etc. is employable.
[0102] For example, in mutual recognition processing which was explained by drawing 7 , if it is checked that mutual is a just device next, to the ENI cast address information which received from the address output former portable mold storage 801, an ENI cast address selection processor performs electronic signature by private key Kpri-W of self, and further, it will encipher by public key Kpub-Sn of the portable mold storage acquired on the occasion of previous authentication processing, and it will transmit it to the address output point portable mold storage 802. In addition, although this example explains the example which applied a partner's public key as a key for encryption processing in the data communication between mutual devices, it is good also as a configuration which performs a communication link data encryption using the session key shared at the time of the mutual recognition in a public key cryptosystem.
[0103] After the address output point portable mold storage 802 which received the enciphered ENI cast address information performs decode processing for received data by private key Kpri-Sn of self, it performs verification of electronic signature to ENI cast address information with the application of public key Kpub-W of an ENI cast address selection processor, and judges the existence of an alteration. In addition, although electronic signature is explained as an example currently made with the private key of an ENI cast address selection processor, it is good also as a configuration with which the signature is made with other ID issuance engines' private key, and stores the public key of ID issuance engine for signature verification in the portable mold storage which performs signature verification in this case here.
[0104] If it judges with a portable mold storage not having an alteration in ENI cast address information by signature verification, ENI cast address information including electronic signature is stored in the interface ID storing memory 324 at the basis of control of CPU320 shown in drawing 3 . A portable mold storage transmits a confirmation-of-receipt response to an ENI cast address selection processor after these processings. An ENI cast address selection processor receives a confirmation-of-receipt response, and processing is completed.
[0105] Copy processing of the ENI cast address through [copy processing of the ENI cast address through (3) ENI cast address selection processor between different portable mold storages], next an ENI cast address selection processor between different portable mold storages is explained using drawing 10 . The copied material portable mold storage 901 which becomes the copy origin of the ENI cast address, and copy place portable mold storage 902,903 -- which stores the ENI cast address by the copy and starts an activity are connected to an ENI cast address selection processor one by one, and processing is performed.
[0106] The ENI cast address information to which electronic signature was added is written in the memory (interface ID storing memory 324 in drawing 3) of the copied material portable mold storage 901.
[0107] First, between ENI cast address selection processors is connected with the copied material portable mold storage 901 which becomes the copy origin of the ENI cast address, and mutual recognition processing is performed. When it is checked that mutual is a just device, in mutual recognition processing next, the copied material portable mold storage 901 The ENI cast address information written in the memory in a portable mold storage is read. Generate the signature by the self private key and encryption processing of transmit data is further performed using the public key of the ENI cast address selection processor which is a session key or a communications partner. It transmits to

an ENI cast address selection processor as encryption ENI cast address information with a signature.
[0108] If the ENI cast address information enciphered from the copied material portable mold storage 901 is received, an ENI cast address selection processor performs decode processing with the application of a session key or a self private key, further, will perform signature verification with the application of the public key of a portable mold storage, and will check the existence of a data alteration.
[0109] An ENI cast address selection processor will generate copy A.I. Artificial Intelligence-1 and A.I. Artificial Intelligence-2 by it based on the ENI cast address information (A.I. Artificial Intelligence) which transmits a confirmation-of-receipt response to the copied material portable mold storage 901, and receives further and by which justification was verified, if the justification of data is checked by signature verification of the ENI cast address information which received from the copied material portable mold storage 901 etc.
[0110] In addition, a new correction attribute is added by the copied ENI cast address information (A.I. Artificial Intelligence-n) (electronic signature). The total value of the final count of a copy of all the ENI cast addresses obtained as a result of a copy must be controlled to become equal to the newest count of ENI cast address information which became the beginning the copied material and which can be copied naturally. In this way, two or more ENI cast address information A.I. Artificial Intelligence-1, A.I. Artificial Intelligence-2, and ... are obtained.
[0111] Next, in an ENI cast address selection processor, the copy place portable mold storage 902 of an address copy place is connected. It enciphers with the public key of the portable mold storage which the ENI cast address selection processor performed electronic signature by self private key Kpri-W to the copy (A.I. Artificial Intelligence-2) of the ENI cast address when it was checked that it is [in / if connection is made, authentication processing will be performed, and / authentication processing] a device with mutual [just], and was further acquired on the occasion of previous authentication processing, and transmits to the copy place portable mold storage 902.
[0112] The copy place portable mold storage 902 which received the enciphered ENI cast address information After a self private key performs decode processing for received data, verification of electronic signature to ENI cast address information is performed with the application of public key Kpub-W of an ENI cast address selection processor. If the existence of an alteration is judged and it judges with there being no alteration in ENI cast address information by signature verification, ENI cast address information including electronic signature is stored in the interface ID storing memory 324 at the basis of control of CPU320 shown in drawing 3 . A portable mold storage transmits a confirmation-of-receipt response to an ENI cast address selection processor after these processings.
[0113] Furthermore, in an ENI cast address selection processor, the copy place portable mold storage 903 of an address copy place is connected, and the same processing is repeated. These processings are repeatedly performed according to the number of the portable mold storages used as a copy place.
[0114] [Utilization processing of (4) ENI cast address], next utilization processing of the ENI cast address are explained using drawing 11 . When a user actually performs an IPv6 communication link, transfer of the temporary address is performed between the portable mold storages which stored the user terminal and the ENI cast address as a communication terminal. It is because a user terminal applies a correction attribute to ENI cast address information according to a utilization situation and processing returned to a portable mold storage is performed, after restricting the reason for having written that it was temporary to IPv6 communication link utilization time, and a portable mold storage's eliminating the ENI cast address from a delivery portable mold storage to a user terminal and completing an IPv6 communication link. The unexpected simultaneous activity about the same ENI cast address information is prevented by carrying out like this.
[0115] Utilization processing of the ENI cast address is explained with reference to drawing 11 . The ENI cast address information to which electronic signature was added is written in the memory (interface ID storing memory 324 in drawing 3) of the portable mold storage which becomes the offer origin of the ENI cast address. A communication plug and a communication link socket connect and the user terminal

as a portable mold storage and a communication terminal is in the condition in which data transfer is possible.

[0116] First, mutual recognition processing is performed between the portable mold storage which becomes the offer origin of the ENI cast address, and the communication terminal as an ENI cast address utilization terminal. In mutual recognition processing, if it is checked that mutual is a just device next, a communication terminal will require an address transfer of a portable mold storage. A portable mold storage reads the ENI cast address information written in the memory in a portable mold storage, generates the signature by the self private key, performs encryption processing of transmit data further using the public key of the communication terminal which is a session key or a communications partner, and transmits it to a communication terminal as encryption ENI cast address information with a signature.

[0117] If the ENI cast address information enciphered from the portable mold storage is received, a communication terminal performs decode processing with the application of a session key or a self private key, further, will perform signature verification with the application of the public key of an address output former portable mold storage, and will check the existence of a data alteration.

[0118] Furthermore, a communication terminal performs the count of a copy, utilization-time verification, etc. by attribute verification of the ENI cast address information which received from the portable mold storage. These are the same processings as steps S108 and S109 previously explained using drawing 9 . A check of the justification of data transmits a confirmation-of-receipt response to a portable mold storage. A portable mold storage performs elimination processing of the ENI cast address based on an Acknowledgement.

[0119] A communication terminal stores in self memory (interface ID storing memory 318 in drawing 3) the ENI cast address information which received from the portable mold storage, and starts communications processing as the ENI cast address of self. In addition, when utilization time setting is made like the IPv6 ENI cast address in this case, utilization-time measurement using RTC is performed.

[0120] After communications processing is completed, based on the measured utilization time, a correction attribute is generated and it signs with the private key of further self. Then, it enciphers with the public key of a portable mold storage, and transmits to a portable mold storage.

[0121] The portable mold storage which received the enciphered ENI cast address information After a self private key performs decode processing for received data, verification of electronic signature to ENI cast address information is performed with the application of the public key of a communication terminal. If the existence of an alteration is judged and it judges with there being no alteration in ENI cast address information by signature verification, ENI cast address information including electronic signature is stored in the interface ID storing memory 324 at the basis of control of CPU320 shown in drawing 3 . After these processings, a portable mold storage transmits a confirmation-of-receipt response to a communication terminal, and ends processing.

[0122] By these processings, the correction attribute by utilization of a communication terminal will be applied to the ENI cast address information stored in a portable mold storage at any time, and will be stored in it.

[0123] The detail of [(5) ENI cast address return (recovery) processing], next ENI cast address return (recovery) processing is explained. Drawing which explains the processing sequence in ENI cast address return (recovery) processing to drawing 12 is shown. A portable mold storage here is a device which returns the ENI cast address.

[0124] Electronic signature is added to the memory of a portable mold storage, and the ENI cast address is written in it. The mutual one between ENI cast address selection processors is connected with the portable mold storage which returns the ENI cast address, and mutual recognition processing is performed.

[0125] In mutual recognition processing, if it is checked that mutual is a just device next, a portable mold storage will read the ENI cast address written in memory, and will transmit it to an ENI cast

address selection processor. An ENI cast address selection processor will perform deletion of the data registered into the ENI cast address administration database as nullification processing of the ENI cast address a condition [the check of there being no alteration of the ENI cast address by verification of electronic signature], if the ENI cast address is received from a portable mold storage. An ENI cast address administration database is a database for issuance management of the ENI cast address, and deletes the matching data of the ENI cast address, expiration date management data, etc. with a user.
[0126] Then, an ENI cast address selection processor transmits advice of the completion of ENI cast address recovery processing to a portable mold storage, and the portable mold storage which received advice of completion performs elimination processing of the ENI cast address written in self memory.
[0127] In addition, two or more ENI cast addresses can be written in a portable mold storage if needed. For example, in order to use different services, such as ENI cast service, by one or more IPv6 devices, it is possible to store and use two or more ENI cast addresses for a portable mold storage. By holding two or more ENI cast addresses to a portable mold storage, service of various quality and functions can be related with each ENI cast address. For example, by storing in a portable mold storage by making into the ENI cast address the ENI cast address which applies application service of a TV phone, a user terminal can also receive TV phone service now using the ENI cast address X.
[0128] As mentioned above, it has explained in detail about this invention, referring to a specific example. However, it is obvious that this contractor can accomplish correction and substitution of this example in the range which does not deviate from the summary of this invention. That is, with the gestalt of instantiation, this invention has been indicated and it should not be interpreted restrictively. In order to judge the summary of this invention, the column of the claim indicated at the beginning should be taken into consideration.
[0129] In addition, a series of processings in which it explained into the description can be performed by the compound configuration of hardware and software both. As for the processing by software, it is possible to install the program which recorded the processing sequence in the memory in the computer built into the hardware of dedication, and to perform it, or to make the general purpose computer which can perform various processings install and execute a program.
[0130] For example, a program is recordable on the hard disk and ROM (Read OnlyMemory) as a record medium beforehand. Or a program is permanently [temporarily or] storable in removable record media, such as a floppy (trademark) disk, CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) disk, DVD (Digital Versatile Disc), a magnetic disk, and semiconductor memory, (record). Such a removable record medium can be offered as the so-called software package.
[0131] In addition, a program is installed in a computer from a removable record medium which was mentioned above, and also it is installable in record media, such as a hard disk which carries out a wireless transfer, or transmits to a computer with a cable through networks, such as LAN (Local Area Network) and the Internet, at a computer, receives the program transmitted by making it such by computer, and is built in from a download site. In addition, various kinds of processings indicated by the description meet the throughput or need for equipment of time series not only performing, but performing processing according to a publication, and may be performed in juxtaposition or individually.

[0132]
[Effect of the Invention] As mentioned above, as explained, according to the computer program, the ENI cast address was made available with various communication terminals by distributing the ENI cast address using a portable mold storage at the address managerial system of this invention, an ENI cast address selection processor, a communication terminal, information enclosure and the address management method, and the list. Since the ENI cast address becomes eternal to replacement of a device, an IPv6 communication link can be used for high service of availability, such as a telephone. Moreover, it becomes possible to use the ENI cast address as an identifier of a user proper, and becomes useful as an infrastructure of customer individual response mold service.

[0133] Furthermore, processing of migration of the ENI cast address, a copy, return, etc. is possible, a belt can be performed using the address, and efficient utilization of the ENI cast address is attained. Moreover, by having solved safety required for an exchange of the ENI cast address using the digital contents protection feature, it cannot come out of an exchange of the ENI cast address to insurance as much as possible, the common device corresponding to a portable mold storage can perform, and a user's convenience increases. Moreover, it becomes possible to exclude the activity which inputs write-in processing of the ENI cast address etc. with a help, the ENI cast address can be distributed correctly easily, and a user's convenience increases.

[0134] Furthermore, since two or more ENI cast addresses can be held to a portable mold storage, service of various quality and functions can be related with each ENI cast address. Two or more ENI cast services can be made by this to be able to offer to a highly efficient communication terminal, and a product can be differentiated. For example, when a voice telephone is given to the ENI cast address A and the attribute of a TV phone is given to the ENI cast address B, address utilization processing in which Address A is distributed to an audio terminal and Addresses A and B are distributed to a TV phone terminal using a portable mold storage is attained.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－51837
（P2003－51837A）
(43)公開日　平成15年２月21日(2003.2.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｂ	５Ｂ０８５
// Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｋ０３０

審査請求　未請求　請求項の数31　ＯＬ　（全 22 頁）

(21)出願番号　特願2001－239147(P2001－239147)

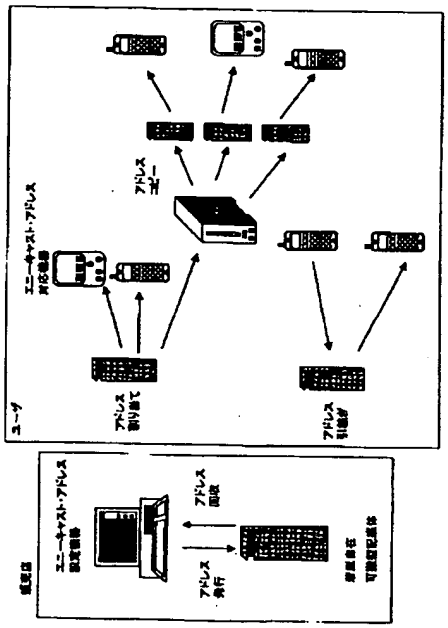
(22)出願日　平成13年８月７日(2001.8.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　三好　寛
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　宮内　敦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　アドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】　可搬型記憶媒体を利用した改善されたアドレス管理処理システムを提供する。
【解決手段】　可搬型記憶媒体を用いてエニーキャスト・アドレスを配布することで、エニーキャスト・アドレスを様々な通信端末装置で利用可能とした。エニーキャスト・アドレスは機器の置き換えに対して不変となるので、電話等の可用性の高いサービスにＩＰｖ６通信を利用できるようになる。また、エニーキャスト・アドレスをユーザ固有の識別子として用いることが可能となり、顧客個別対応型サービスのインフラストラクチャとして有用となる。さらに、エニーキャスト・アドレスの移動、コピー、返却等の処理が可能であり、アドレスの使いまわしを行うことができ、エニーキャスト・アドレスの効率的な利用が可能となる。



1

【特許請求の範囲】

【請求項１】通信処理を実行する通信端末に設定するアドレスの管理を行なうアドレス管理システムであり、

アドレス設定対象となる通信端末と、

前記通信端末に装着し、エニーキャスト・アドレスを格納する可搬型記憶媒体と、

該通信端末に対応するアドレスとしてのエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置とを有し、

前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、エニーキャスト・アドレス情報を前記可搬型記憶媒体に出力し、

前記エニーキャスト・アドレス情報を受信した可搬型記憶媒体は、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報を格納し、接続された通信端末との認証成立を条件として、エニーキャスト・アドレス情報を前記通信端末に出力し、

前記通信端末は、前記可搬型記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とするアドレス管理システム。

【請求項２】前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする請求項１に記載のアドレス管理システム。

【請求項３】前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力し、

前記エニーキャスト・アドレス情報および電子署名を受信した可搬型記憶媒体は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報および電子署名を格納することを特徴とする請求項１に記載のアドレス管理システム。

【請求項４】可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報には改竄検証用の電子署名が付加された構成であることを特徴とする請求項１に記載のアドレス管理システム。

【請求項５】可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報のデータ変更時には更新データからなる修正属性が生成されるとともに、該修正属性を生成した機器による電子署名を付加して可搬型記憶媒体に格納する構成であることを特徴とする請求項１に記載のアドレス管理システム。

【請求項６】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする請求項１に記載のアドレス管理システム。

2

【請求項７】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第２の通信端末に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする請求項１に記載のアドレス管理システム。

【請求項８】前記可搬型記憶媒体は、通信端末との認証成立を条件として、エニーキャスト・アドレス情報に電子署名を付加して通信端末に出力し、

前記エニーキャスト・アドレス情報および電子署名を受信した通信端末は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とする請求項１に記載のアドレス管理システム。

【請求項９】前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行する構成を有することを特徴とする請求項１に記載のアドレス管理システム。

【請求項１０】通信端末に対応するアドレスとしてのエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置であり、

アドレス格納対象となる可搬型記憶媒体との認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報を出力する構成を有することを特徴とするエニーキャスト・アドレス設定処理装置。

【請求項１１】前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１２】前記エニーキャスト・アドレス設定処理装置は、さらに、

可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力する構成であることを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１３】前記エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレス情報に、利用条件を含む属性情報を含ませ、該属性情報に改竄検証用の電子署名を付加して可搬型記憶媒体に出力する構成であることを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１４】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１５】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１６】前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行する構成を有することを特徴とする請求項１０に記載のエニーキャスト・アドレス設定処理装置。

【請求項１７】通信処理を実行する通信端末装置であり、

通信端末に対応するアドレスを含むエニーキャスト・アドレス情報を、該通信端末装置に装着した可搬型記憶媒体との認証成立を条件として、可搬型記憶媒体から受信し、前記エニーキャスト・アドレス情報に対して生成された電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とする通信端末装置。

【請求項１８】前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする請求項１７に記載の通信端末装置。

【請求項１９】通信端末装置に対して着脱自在な構成を有し、データ処理機能を有する情報格納装置であり、

通信端末装置に対応するアドレスを含むエニーキャスト・アドレス情報をメモリに格納し、該通信端末装置との認証成立を条件として、前記エニーキャスト・アドレス情報を情報格納装置のメモリから読み出して通信端末装置に出力する構成を有することを特徴とする情報格納装置。

【請求項２０】前記情報格納装置は、

前記エニーキャスト・アドレス情報を情報格納装置のメモリから読み出して通信端末装置に出力するとともに、

前記エニーキャスト・アドレス情報を情報格納装置のメモリから消去する処理を実行する構成を有することを特徴とする請求項１９に記載の情報格納装置。

【請求項２１】通信処理を実行する通信端末に設定するアドレスの管理を行なうアドレス管理方法であり、

エニーキャスト・アドレス設定処理装置と可搬型記憶媒体との認証成立を条件として、エニーキャスト・アドレス情報をエニーキャスト・アドレス設定処理装置から可搬型記憶媒体に出力するステップと、

前記エニーキャスト・アドレス情報を受信した可搬型記憶媒体が、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報を格納するステップと、

可搬型記憶媒体と通信端末との認証成立を条件として、可搬型記憶媒体からエニーキャスト・アドレス情報を前記通信端末に出力するステップと、

前記通信端末において、前記可搬型記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定するステップと、

を有することを特徴とするアドレス管理方法。

【請求項２２】前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２３】前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力し、

前記エニーキャスト・アドレス情報および電子署名を受信した可搬型記憶媒体は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報および電子署名を格納することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２４】可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報には改竄検証用の電子署名が付加された構成であることを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２５】可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付

加されて格納され、該属性情報のデータ変更時には更新データからなる修正属性が生成されるとともに、該修正属性を生成した機器による電子署名を付加して可搬型記憶媒体に格納することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２６】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２７】前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２８】前記可搬型記憶媒体は、通信端末との認証成立を条件として、エニーキャスト・アドレス情報に電子署名を付加して通信端末に出力し、

前記エニーキャスト・アドレス情報および電子署名を受信した通信端末は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項２９】前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行することを特徴とする請求項２１に記載のアドレス管理方法。

【請求項３０】通信端末に設定するアドレスの発行を行なうアドレス発行処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

通信端末に対応するアドレスを含むエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置と、アドレスを格納する情報格納装置間での認証処理ステップと、

認証成立を条件として、エニーキャスト・アドレス設定処理装置から情報格納装置に対してエニーキャスト・アドレス情報を出力するステップと、

情報格納装置において、エニーキャスト・アドレス情報に対する電子署名検証処理を実行し、改竄無しの確認を条件としてメモリに格納するステップと、

を具備することを特徴とするコンピュータ・プログラム。

【請求項３１】通信端末に設定されるアドレスの利用による通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

通信端末装置と通信端末装置に装着された記憶媒体間における認証処理ステップと、

記憶媒体と通信端末との認証成立を条件として、記憶媒体からエニーキャスト・アドレス情報を前記通信端末に出力するステップと、

前記通信端末において、前記記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定するステップと、

を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムに関する。さらに詳細には、ＩＰｖ６(Internet Protocol version 6)におけるインタフェースＩＤの機器間でのスムースな受け渡しを可能としたアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の通信端末装置を携帯し、屋外であるいは移動先においてネットワークに接続してネットワークを介する通信を行なっている。

【０００３】インターネットでは通信プロトコルとしてＩＰ(Internet Protocol)が用いられている。現在多く使用されているＩＰはＩＰｖ４であり、発信元／宛先として３２ビットからなるアドレス（ＩＰアドレス）が用いられている。インターネット通信においては、３２ビットＩＰアドレスを各発信元／宛先にユニークに割り当てるグローバルＩＰアドレスを採用し、ＩＰアドレスに応じて、個々の発信元／宛先を判別している。しかし、インターネットの世界は急速に広がりを見せており、ＩＰｖ４の限られたアドレス空間、すなわちグローバルアドレスの枯渇が問題となってきている。これを解決するためにＩＥＴＦ（Internet Engineering Task Force）では、次世代ＩＰアドレスとしてＩＰアドレス空間を３２ビットから１２８ビットに拡張する新しいＩＰｖ６(Internet Protocol version 6)を提案している。

【０００４】ＩＰｖ６は現行のＩＰｖ４の後継プロトコルであり、図１に示すアドレス形式を有する。ＩＰｖ６は１２８ビット構成であり、下位ビットがインターネット上、もしくはサブネット上でノードを一意に識別するためのノード識別子としてのインタフェースＩＤ(Interface ID)(例えばＩＥＥＥ８０２形式)であり、上位ビットがノードが接続しているサブネットワークを示す位置指示子としてのネットワークプレフィックス（Network Prefix）である。従って、基本的に同一のサブネットワークに属する端末装置は、ＩＰｖ６アドレスの上位ビットの示すネットワークプレフィックス（Network Prefix）が同一なものとなる。

【０００５】ＩＰｖ６ではパケットの配送はプレフィクスおよびサブネット番号のみに基づいて行われるため、それより下位のアドレス、すなわちインタフェースＩＤは機器製造メーカにおいて割り当てが可能となる。正確にはインタフェースＩＤ番号の一部が製造メーカ識別子であり、残った部分がメーカの裁量に委ねられる。従ってＩＰｖ４と異なり、ＩＰｖ６では、インタフェースＩＤすなわちＩＰｖ６アドレスの一部をメーカが自由に決定することができ、それを例えばユーザＩＤに対応付けることで、発売した機器と顧客情報をインタフェースＩＤを介して結び付けることが可能となる。

【０００６】ところが、現実にはインタフェースＩＤと顧客との対応は固定的ではなく、変動するものとなる。これは、例えばユーザによる端末の買い替えなどの顧客行動に起因する。このようなインタフェースＩＤと顧客との対応関係の変動は、ＩＰ電話のようにユーザとＩＰアドレスを対応付けて利用するアプリケーションに悪影響を及ぼす。例えばＩＰ電話の場合、電話相手の汎用名を示すデータと、実際の通信相手機器のＩＰアドレスとの対応データをアドレス解決機構として保持し、この対応データに基づいてサービスを提供することが行われる。

【０００７】しかし、ユーザによる端末買い替えなどの顧客行動によりインタフェースＩＤとユーザの対応関係が変わった場合は、対応データの修正処理が完了するまでは、買い替えた機器による通信は出来ない。何故ならパケット配送はプレフィクス及びサブネット番号に基づくか、配送の最後にＩＰｖ６機器はインタフェースＩＤを含むＩＰｖ６アドレス全体を比較してパケットを受信するか否かを決定するからである。

【０００８】このような状況は、電話のように極めて強い可用性が要求される用途では回避されることが望ましい。従来の構成においては、携帯電話のように高い可用性を要求される用途に対して、インタフェースＩＤと顧客の対応関係が崩れる可能性のあるＩＰｖ６を適用することは難しいと考えられていた。

【０００９】

【発明が解決しようとする課題】本発明は、従来構成における上述の問題点に鑑みてなされたものであり、ＩＰｖ６のエニーキャスト機構をユーザ固有のＩＤとして扱うことで、ユーザ個別のサービスを提供可能な環境を作り、利便性を高めるアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムを提供する。

【００１０】ＩＰｖ６のアドレスでは、ユニキャスト、エニーキャスト、マルチキャストの３種類のアドレスを定義している。ユニキャストは、単一のインタフェースを指示する識別子であり、パケットは、ユニキャスト・アドレスの示す単一のインタフェースに配送される。エニーキャストは複数のインタフェースの集合を指す識別子であり、そのアドレスの示すインタフェースから、経路制御プロトコルによる距離測定に基づいて選択される最も近い１つのインタフェースにパケットが配送される。マルチキャストは、複数のインタフェースの集合を指す識別子であり、そのアドレスの示すすべてのインタフェースにパケットが配送される。

【００１１】エニーキャストとは、複数の端末に対してサービス要求を出し、それらのうちの１つ以上がサービスを行うモデルで、所謂、代表電話サービスのようなものである。このときの代表電話番号のＩＰｖ６版がエニーキャスト・アドレスである。

【００１２】エニーキャスト・アドレスをユーザ固有のものとして扱うことで、全ての機器に共通のアドレスを割り付けることができ、機器の変更の際にそのアドレスを変更する必要がなくなる。この手法は、エニーキャスト型サービスも同時に実現できる等の利点も持つため有望である。

【００１３】本発明においては、ディジタルコンテンツ保護機構を有する可搬型記憶装置を利用することで不正なＩＤ使用を防止しつつ面倒なＩＤ設定を簡単に行なうことのできるアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明の第１の側面は、通信処理を実行する通信端末に設定するアドレスの管理を行なうアドレス管理システムであり、アドレス設定対象となる通信端末と、前記通信端末に装着し、エニーキャスト・アドレスを格納する可搬型記憶媒体と、該通信端末に対応するアドレスとしてのエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置とを有し、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、エニーキャスト・アドレス情報を前記可搬型記憶媒体に出力し、前記エニーキャスト・アドレス情報を受信した可搬型記憶媒体は、可搬型記憶媒体内のメモリに受信エニー

キャスト・アドレス情報を格納し、接続された通信端末との認証成立を条件として、エニーキャスト・アドレス情報を前記通信端末に出力し、前記通信端末は、前記可搬型記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とするアドレス管理システムにある。

【００１５】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする。

【００１６】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力し、前記エニーキャスト・アドレス情報および電子署名を受信した可搬型記憶媒体は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報および電子署名を格納することを特徴とする。

【００１７】さらに、本発明のアドレス管理システムの一実施態様において、可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報には改竄検証用の電子署名が付加された構成であることを特徴とする。

【００１８】さらに、本発明のアドレス管理システムの一実施態様において、可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報のデータ変更時には更新データからなる修正属性が生成されるとともに、該修正属性を生成した機器による電子署名を付加して可搬型記憶媒体に格納する構成であることを特徴とする。

【００１９】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする。

【００２０】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第２の通信端末に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする。

【００２１】さらに、本発明のアドレス管理システムの一実施態様において、前記可搬型記憶媒体は、通信端末との認証成立を条件として、エニーキャスト・アドレス情報に電子署名を付加して通信端末に出力し、前記エニーキャスト・アドレス情報および電子署名を受信した通信端末は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とする。

【００２２】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行する構成を有することを特徴とする。

【００２３】さらに、本発明の第２の側面は、通信端末に対応するアドレスとしてのエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置であり、アドレス格納対象となる可搬型記憶媒体との認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報を出力する構成を有することを特徴とするエニーキャスト・アドレス設定処理装置にある。

【００２４】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス情報に含まれるアドレスはＩＰｖ６において規定するアドレス構造における下位ビットを構成するインタフェースＩＤであることを特徴とする。

【００２５】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、さらに、可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力する構成であることを特徴とする。

【００２６】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレス情報に、利用条件を含む属性情報を含ませ、該属性情報に改竄検証用の電子署名を付加して可搬型記憶媒体に出力する構成であることを特徴とする。

【００２７】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする。

【0028】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第1の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第2の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする。

【0029】さらに、本発明のエニーキャスト・アドレス設定処理装置の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行する構成を有することを特徴とする。

【0030】さらに、本発明の第3の側面は、通信処理を実行する通信端末装置であり、通信端末に対応するアドレスを含むエニーキャスト・アドレス情報を、該通信端末装置に装着した可搬型記憶媒体との認証成立を条件として、可搬型記憶媒体から受信し、前記エニーキャスト・アドレス情報に対して生成された電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定する構成を有することを特徴とする通信端末装置にある。

【0031】さらに、本発明の通信端末装置の一実施態様において、前記エニーキャスト・アドレス情報に含まれるアドレスはIPv6において規定するアドレス構造における下位ビットを構成するインタフェースIDであることを特徴とする。

【0032】さらに、本発明の第4の側面は、通信端末装置に対して着脱自在な構成を有し、データ処理機能を有する情報格納装置であり、通信端末装置に対応するアドレスを含むエニーキャスト・アドレス情報をメモリに格納し、該通信端末装置との認証成立を条件として、前記エニーキャスト・アドレス情報を情報格納装置のメモリから読み出して通信端末装置に出力する構成を有することを特徴とする情報格納装置にある。

【0033】さらに、本発明の情報格納装置の一実施態様において、前記情報格納装置は、前記エニーキャスト・アドレス情報を情報格納装置のメモリから読み出して通信端末装置に出力するとともに、前記エニーキャスト・アドレス情報を情報格納装置のメモリから消去する処理を実行する構成を有することを特徴とする。

【0034】さらに、本発明の第5の側面は、通信処理を実行する通信端末に設定するアドレスの管理を行なうアドレス管理方法であり、エニーキャスト・アドレス設定処理装置と可搬型記憶媒体との認証成立を条件として、エニーキャスト・アドレス情報をエニーキャスト・アドレス設定処理装置から可搬型記憶媒体に出力するステップと、前記エニーキャスト・アドレス情報を受信した可搬型記憶媒体が、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報を格納するステップと、可搬型記憶媒体と通信端末との認証成立を条件として、可搬型記憶媒体からエニーキャスト・アドレス情報を前記通信端末に出力するステップと、前記通信端末において、前記可搬型記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定するステップと、を有することを特徴とするアドレス管理方法にある。

【0035】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス情報に含まれるアドレスはIPv6において規定するアドレス構造における下位ビットを構成するインタフェースIDであることを特徴とする。

【0036】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の認証成立を条件として、可搬型記憶媒体に格納するエニーキャスト・アドレス情報に電子署名を付加して出力し、前記エニーキャスト・アドレス情報および電子署名を受信した可搬型記憶媒体は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、可搬型記憶媒体内のメモリに受信エニーキャスト・アドレス情報および電子署名を格納することを特徴とする。

【0037】さらに、本発明のアドレス管理方法の一実施態様において、可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報には改竄検証用の電子署名が付加された構成であることを特徴とする。

【0038】さらに、本発明のアドレス管理方法の一実施態様において、可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には、利用条件を含む属性情報が付加されて格納され、該属性情報のデータ変更時には更新データからなる修正属性が生成されるとともに、該修正属性を生成した機器による電子署名を付加して可搬型記憶媒体に格納することを特徴とする。

【0039】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第1の可搬型記憶媒体から受理したエニーキャスト・アドレス情報を、他の第2の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行することを特徴とする。

【0040】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス設定処

理装置は、接続した第1の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第2の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行することを特徴とする。

【0041】さらに、本発明のアドレス管理方法の一実施態様において、前記可搬型記憶媒体は、通信端末との認証成立を条件として、エニーキャスト・アドレス情報に電子署名を付加して通信端末に出力し、前記エニーキャスト・アドレス情報および電子署名を受信した通信端末は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定することを特徴とする。

【0042】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行することを特徴とする。

【0043】さらに、本発明の第6の側面は、通信端末に設定するアドレスの発行を行なうアドレス発行処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、通信端末に対応するアドレスを含むエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置と、アドレスを格納する情報格納装置間での認証処理ステップと、認証成立を条件として、エニーキャスト・アドレス設定処理装置から情報格納装置に対してエニーキャスト・アドレス情報を出力するステップと、情報格納装置において、エニーキャスト・アドレス情報に対する電子署名検証処理を実行し、改竄無しの確認を条件としてメモリに格納するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【0044】さらに、本発明の第7の側面は、通信端末に設定されるアドレスの利用による通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、通信端末装置と通信端末装置に装着された記憶媒体間における認証処理ステップと、記憶媒体と通信端末との認証成立を条件として、記憶媒体からエニーキャスト・アドレス情報を前記通信端末に出力するステップと、前記通信端末において、前記記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【0045】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0046】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0047】

【発明の実施の形態】以下、本発明のアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法について、図面を参照しながら詳細に説明する。

【0048】図2を用いて、本発明のアドレス管理システムの概要を説明する。本発明のアドレス管理システムにおいて、アドレス（IPv6アドレス）を用いてデータ通信を実行する機器は通信機能を有する通信端末装置としてのユーザ端末130であり、これは例えば携帯電話、PDAなどの機器である。これらのユーザ端末は、例えばIP電話のようにユーザとIPアドレスを対応付けたアプリケーション利用処理が可能である。

【0049】ユーザ端末130は、例えばフラッシュメモリを搭載した可搬型記憶媒体120を着脱可能な構成を持つ。なお、可搬型記憶媒体120はCPUを有しメモリに対する情報格納、消去、読み出しをCPUの制御の下に行なう情報処理可能な情報格納装置である。エニーキャスト・アドレス設定処理装置110と可搬型記憶媒体120との間でデータ転送を実行することで、IPv6エニーキャスト・アドレスの下位ビットアドレスであるインタフェースIDをエニーキャスト・アドレス設定処理装置110から可搬型記憶媒体120に受信格納する。ユーザ端末130は、エニーキャスト・アドレス（インタフェースID）を格納した可搬型記憶媒体120を装着することで、可搬型記憶媒体120に格納したエニーキャスト・アドレス（インタフェースID）をユーザ端末130のアドレスとして利用する。

【0050】なお、本実施例では、IPv6アドレスのインタフェースIDをエニーキャスト用途で用いることを前提とする。以下、エニーキャスト・アドレスという言葉でインタフェースIDを指すものとする。IPv6本来の定義のエニーキャスト・アドレスは、インタフェ

理装置は、接続した第1の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第2の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行することを特徴とする。

【0041】さらに、本発明のアドレス管理方法の一実施態様において、前記可搬型記憶媒体は、通信端末との認証成立を条件として、エニーキャスト・アドレス情報に電子署名を付加して通信端末に出力し、前記エニーキャスト・アドレス情報および電子署名を受信した通信端末は、電子署名の検証による、受信データの改竄の無いことの確認を条件として、通信端末内のメモリに受信エニーキャスト・アドレス情報を格納して該通信端末対応エニーキャスト・アドレスとして設定することを特徴とする。

【0042】さらに、本発明のアドレス管理方法の一実施態様において、前記エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体から電子署名のなされたエニーキャスト・アドレス情報を受信し、該電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報の回収処理として、エニーキャスト・アドレス情報管理データベースからのデータ削除処理を実行することを特徴とする。

【0043】さらに、本発明の第6の側面は、通信端末に設定するアドレスの発行を行なうアドレス発行処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、通信端末に対応するアドレスを含むエニーキャスト・アドレス情報を発行するエニーキャスト・アドレス設定処理装置と、アドレスを格納する情報格納装置間での認証処理ステップと、認証成立を条件として、エニーキャスト・アドレス設定処理装置から情報格納装置に対してエニーキャスト・アドレス情報を出力するステップと、情報格納装置において、エニーキャスト・アドレス情報に対する電子署名検証処理を実行し、改竄無しの確認を条件としてメモリに格納するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【0044】さらに、本発明の第7の側面は、通信端末に設定されるアドレスの利用による通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、通信端末装置と通信端末装置に装着された記憶媒体間における認証処理ステップと、記憶媒体と通信端末との認証成立を条件として、記憶媒体からエニーキャスト・アドレス情報を前記通信端末に出力するステップと、前記通信端末において、前記記憶媒体から受信したエニーキャスト・アドレス情報に含まれるアドレスを該通信端末対応エニーキャスト・アドレスとして設定するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【0045】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0046】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0047】

【発明の実施の形態】以下、本発明のアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法について、図面を参照しながら詳細に説明する。

【0048】図2を用いて、本発明のアドレス管理システムの概要を説明する。本発明のアドレス管理システムにおいて、アドレス（IPv6アドレス）を用いてデータ通信を実行する機器は通信機能を有する通信端末装置としてのユーザ端末130であり、これは例えば携帯電話、PDAなどの機器である。これらのユーザ端末は、例えばIP電話のようにユーザとIPアドレスを対応付けたアプリケーション利用処理が可能である。

【0049】ユーザ端末130は、例えばフラッシュメモリを搭載した可搬型記憶媒体120を着脱可能な構成を持つ。なお、可搬型記憶媒体120はCPUを有しメモリに対する情報格納、消去、読み出しをCPUの制御の下に行なう情報処理可能な情報格納装置である。エニーキャスト・アドレス設定処理装置110と可搬型記憶媒体120との間でデータ転送を実行することで、IPv6エニーキャスト・アドレスの下位ビットアドレスであるインタフェースIDをエニーキャスト・アドレス設定処理装置110から可搬型記憶媒体120に受信格納する。ユーザ端末130は、エニーキャスト・アドレス（インタフェースID）を格納した可搬型記憶媒体120を装着することで、可搬型記憶媒体120に格納したエニーキャスト・アドレス（インタフェースID）をユーザ端末130のアドレスとして利用する。

【0050】なお、本実施例では、IPv6アドレスのインタフェースIDをエニーキャスト用途で用いることを前提とする。以下、エニーキャスト・アドレスという言葉でインタフェースIDを指すものとする。IPv6本来の定義のエニーキャスト・アドレスは、インタフェ

ースＩＤにサブネット番号とプレフィクスを加えたＩＰｖ６アドレス全体を指すので、ここで言うエニーキャスト・アドレスとは異なる。ここで言うエニーキャスト・アドレスを、より正確に表現するとすれば、エニーキャスト用途に用意されたインタフェースＩＤとなる。可搬型記憶媒体１２０に格納したインタフェースＩＤは、エニーキャスト用途に用意されたインタフェースＩＤである。

【００５１】エニーキャスト・アドレス設定処理装置１１０は、可搬型記憶媒体１２０と通信し、ユーザ端末１３０の利用可能なエニーキャスト・アドレスを可搬型記憶媒体１２０に対して送信する。可搬型記憶媒体１２０は、エニーキャスト・アドレスを受信してメモリに格納する。

【００５２】エニーキャスト・アドレス設定処理装置１１０は、外部からの要求に応じて新規エニーキャスト・アドレスを生成するエニーキャトスト・アドレス生成手段１１１を有する。ディジタルコンテンツ保護手段１１２は、不正なエニーキャスト・アドレス、不正なアドレス改竄などを検出する。場合によってはそれを修正する機能も有する。ディジタルコンテンツ保護手段１１２は、可搬型記憶媒体１２０との間のエニーキャスト情報転送処理における機器同士の認証やエニーキャスト情報の正当性に関する検査としての電子署名検証、コピー回数制限のチェック、発行元に関する情報のチェック等の処理を実行する。

【００５３】エニーキャスト・アドレス設定処理装置１１０は、内部、または外部にエニーキャスト・アドレス管理データベース１１３を有し、エニーキャトスト・アドレス生成手段１１１におけるエニーキャスト・アドレスの生成時に、エニーキャスト・アドレス管理データベース１１３を参照して重複したエニーキャスト・アドレスの発行がなされないように管理しながら、接続された可搬型記憶媒体１２０に対して、エニーキャスト・アドレスの発行処理を実行する。

【００５４】エニーキャスト・アドレス設定処理装置１１０は、可搬型記憶媒体１２０に対するエニーキャスト・アドレスの発行処理の他に、可搬型記憶媒体１２０からのエニーキャスト・アドレスの回収、あるいは、可搬型記憶媒体１２０内部のエニーキャスト・アドレスを消去する処理を実行する。さらに、必要に応じて、発行、回収、消去したエニーキャスト・アドレスに基づくエニーキャスト・アドレス管理データベース１１３の登録、更新処理を実行する。

【００５５】可搬型記憶媒体１２０は、例えばフラッシュメモリによって構成されるエニーキャスト・アドレス格納手段１２１を有する。エニーキャスト・アドレス格納手段１２１には、ユーザ端末１３０で利用可能なエニーキャスト・アドレス、および、それに関する情報が格納される。例えばエニーキャスト・アドレスの購入者、有効期限、コピー回数、電子署名などの情報が格納される。可搬型記憶媒体１２０に書き込まれるエニーキャスト・アドレスの数は複数とすることが可能である。エニーキャスト・アドレスに関連する情報（たとえばそのアドレスの所有者名や認証のためのキー値、そのアドレスが受け付けるサービス・インタフェースなど）もアドレスと組み合わせて保持可能である。

【００５６】可搬型記憶媒体１２０内のディジタルコンテンツ保護手段１２２は、エニーキャスト・アドレス設定処理装置１１０との間のエニーキャスト情報転送処理における機器同士の認証やエニーキャスト情報の正当性に関する検査としての電子署名検証、コピー回数制限のチェック、発行元に関する情報のチェック等の処理を実行し、さらに、ユーザ端末１３０からのエニーキャスト情報読み取り処理における機器同士の認証やエニーキャスト情報の正当性に関する検査としての電子署名検証、コピー回数制限のチェック、発行元に関する情報のチェック等の処理を実行する。ユーザ端末１３０は、例えばフラッシュメモリを搭載した可搬型記憶媒体１２０を着脱可能な構成を持つ。可搬型記憶媒体１２０を装着することで可搬型記憶媒体１２０のメモリに格納されたエニーキャスト・アドレスを認識し、自己の設定アドレスとして利用するＩＰｖ６対応機器である。通常のＩＰｖ６機器としての使用も可能であり、機器固有のＩＰｖ６対応インタフェースＩＤも有する。

【００５７】ユーザ端末１３０内のエニーキャスト・アドレス利用アプリケーション実行処理手段１３１は、例えばＩＰ電話のようにユーザとＩＰアドレスを対応付けたアプリケーション利用処理を実行する手段、エニーキャスト・アドレスを利用したテレビ電話サービスを実行する手段としてのアプリケーションプログラム実行処理手段である。

【００５８】ユーザ端末１３０内のディジタルコンテンツ保護手段１３２は、エニーキャスト・アドレスを格納した可搬型記憶媒体１２０との間のエニーキャスト情報転送処理における機器同士の認証やエニーキャスト情報の正当性に関する検査としての電子署名検証、コピー回数制限のチェック、発行元に関する情報のチェック等の処理を実行する。

【００５９】次に、図３を用いて、ユーザ端末、可搬型記憶媒体、エニーキャスト・アドレス設定処理装置のハードウェア構成例について説明する。まず、ユーザ端末３１０の構成について説明する。ＣＰＵ(Central processing Unit)３１１は、各種オペレーション、アプリケーションプログラムを実行する。具体的には、ＩＰｖ６の上位層プロトコル処理や端末を操作する人間の入出力操作の処理、および可搬型記憶媒体間で実行されるエニーキャスト・アドレス送受信処理の制御、認証処理等を行なう。ＲＯＭ（Read Only Memory）３１２は、ＣＰＵ３１１が実行するプログラム、あるいは演算パラメータ

としての固定データを格納する。RAM（Random Access Memory）313は、CPU311の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0060】入力部314はCPU311に各種の指令を入力するためにユーザにより操作される。出力部315は例えばLCD（液晶ディスプレイ）等であり、各種情報をテキストまたはイメージ等により表示する。

【0061】IPv6対応インタフェース（I/F）316はIPv6プロトコルを用いて通信可能な通信路を提供する。接続サブネットのルータ等と通信し、CPU311、RAM315等から供給されたデータをパケット化して送信したり、ルータを介してパケットを受信する処理を実行する。RTC317はエニーキャスト・アドレス情報に使用期限を設ける場合に使用するもので必須ではない。RTCはIPv6通信時間を計測する。その時に用いたエニーキャスト・アドレスに付随する使用可能時間から計測時間を減算して修正属性（後述）の形式でエニーキャスト・アドレス情報を更新するために使用する。

【0062】IPv6対応インタフェースID格納メモリ318は、ユーザ端末に設定されたIPv6対応インタフェースIDを格納する不揮発性メモリとして実現され、ユーザ端末の電源が落ちた状態でも消去されない。データの読み書きはCPU311により制御される。通信ソケット319は、可搬型記憶媒体との通信用インタフェースである。

【0063】次に、可搬型記憶媒体320の構成について説明する。CPU(Central processing Unit)321は、各種オペレーション、アプリケーションプログラムを実行する。具体的には、可搬型記憶媒体のメモリに対するデータ格納読み出し制御、データ暗号化、復号処理、署名生成、検証処理、ユーザ端末、あるいはエニーキャスト・アドレス設定処理装置間で実行されるエニーキャスト・アドレス送受信処理の制御、認証処理等を行なう。ROM（Read-Only-Memory）322は、CPU311が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM（Random Access Memory）323は、CPU321の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0064】インタフェースID格納メモリ324は、エニーキャスト・アドレス設定処理装置から受信したIPv6対応エニーキャスト・アドレス（インタフェースID）を格納する不揮発性メモリとして実現される。データの格納、読み出し、消去は、CPU(Central processing Unit)321の制御で実行される。

【0065】通信プラグ325は、ユーザ端末との通信を実行して、エニーキャスト・アドレスの読み出しを可能とするインタフェースあり、またエニーキャスト・アドレス設定処理装置330と接続して、エニーキャスト・アドレスの新規発行処理、回収処理、消去処理を実行する際に用いる通信路を設定するインタフェースである。

【0066】次に、エニーキャスト・アドレス設定処理装置330の構成について説明する。CPU(Central processing Unit)331は、各種オペレーション、アプリケーションプログラムを実行する。具体的には、可搬型記憶媒体320との間で実行されるエニーキャスト・アドレス送受信処理の制御、認証処理等を行なう。ROM（Read-Only-Memory）332は、CPU331が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM（Random Access Memory）333は、CPU331の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0067】入力部334はCPU331に各種の指令を入力するためにユーザにより操作される。出力部335は例えばCRT、LCD（液晶ディスプレイ）等であり、各種情報をテキストまたはイメージ等により表示する。

【0068】エニーキャスト・アドレス管理データベース336は、エニーキャスト・アドレスの発行管理用のデータベースであり、ユーザ、機器とエニーキャスト・アドレスの対応付けデータ、有効期限管理データ等を格納する。なお、この例では、エニーキャスト・アドレス管理データベース336をエニーキャスト・アドレス設定処理装置330内部に構成した例を示しているが、データベースをネットワーク接続外部データベースとして構成し、複数のエニーキャスト・アドレス設定処理装置で共有する構成としてもよい。

【0069】通信ソケット337は、可搬型記憶媒体320と接続して、エニーキャスト・アドレスの新規発行処理、回収処理、消去処理を実行する際に用いる通信路を設定するインタフェースである。

【0070】次に、図4を用いて、本発明のアドレス管理システムにおける具体的な処理例の概要を説明する。ここではある会社がエニーキャスト・アドレスを単品販売するものとし、その販売を販売店に委託した例として説明する。なお、先に説明したように、アドレス（IPv6アドレス）を利用する機器はユーザ端末であり、これは例えば携帯電話、PDAなどの機器である。ユーザ端末は、エニーキャスト・アドレスを格納した可搬型記憶媒体を装着して、可搬型記憶媒体に格納されたエニーキャスト・アドレスを自己のエニーキャスト・アドレス（インタフェースID）として利用した通信を実行する。可搬型記憶媒体は、エニーキャスト・アドレス設定処理装置に接続することでエニーキャスト・アドレスの

格納、回収、消去が実行される。

【００７１】ユーザ端末、および可搬型記憶媒体は、それぞれ前述したようにディジタルコンテンツ保護手段を有し、他機器との通信処理の際の認証処理、暗号処理に適用するデータ、例えば暗号鍵データがＲＯＭに書き込まれて出荷される。

【００７２】販売店では、エニーキャスト・アドレスを単品販売として、可搬型記憶媒体にエニーキャスト・アドレス書き込み設定処理を行なった後ユーザに提供する。あるいは、ユーザの持ち込んだ可搬型記憶媒体にエニーキャスト・アドレス書き込み設定処理を行なう。この処理を実行するのがエニーキャスト・アドレス設定処理装置であり、図２または図３で説明したように、エニーキャスト・アドレスの格納対象となる可搬型記憶媒体とエニーキャスト・アドレス設定処理装置とを接続して、認証処理の成立を条件としてエニーキャスト・アドレス格納処理が実行される。

【００７３】販売店では、新規エニーキャスト・アドレス発行処理のみならず、可搬型記憶媒体に格納済みのエニーキャスト・アドレスの回収処理、さらに、可搬型記憶媒体に格納済みのエニーキャスト・アドレスの消去処理を実行する。

【００７４】販売店はエニーキャスト・アドレス設定処理装置を保有し、顧客がエニーキャスト・アドレスを購入するときにエニーキャスト・アドレス設定処理装置を用いて、顧客の可搬型記憶媒体にエニーキャスト・アドレスを書き込む。このとき同時に顧客に関する種々の情報を新規発行したエニーキャスト・アドレスと組み合わせてエニーキャスト・アドレス設定処理装置および可搬型記憶媒体に登録する。可搬型記憶媒体としては例えばメモリースティックなどのディジタルコンテンツ保護機構を有する機器である。

【００７５】エニーキャスト・アドレス設定処理装置および可搬型記憶媒体に登録するエニーキャスト・アドレス情報の内容を図５に示す。図５の左側は可搬型記憶媒体（Ｓ）に格納されたエニーキャスト・アドレス情報の様子を示したものであり、複数のエニーキャスト・アドレス情報を１つの可搬型記憶媒体（Ｓ）に格納できることを示している。その中の１つのエニーキャスト・アドレス情報について詳細に示したのが図の右側である。エニーキャスト情報は、最低でもＩＰｖ６エニーキャスト・アドレスＡＡと、その生成者が付与するディジタル署名ＳＯ、初期属性ＡＴ１、属性の設定者が付与するディジタル署名ＳＡ１を有する。図の例では、属性としてコピー可能数と利用可能時間の２つを示しているが、属性の種類や数は適宜変更可能であり属性の設定者が必要情報を格納する。

【００７６】コピー利用可能数はＩＰｖ６エニーキャスト・アドレスＡＡを幾つの可搬型記憶媒体に分割コピーして保存して良いかのコピー許可上限を示すコピー制限数である。利用可能時間はＩＰｖ６エニーキャスト・アドレスＡＡを利用できる時間の長さである。この情報は、ユーザ端末に構成されたＲＴＣにより計測されるＩＰｖ６通信時間に従って、使用可能時間から計測時間が減算され更新される。

【００７７】ＩＰｖ６エニーキャスト・アドレスＡＡのコピー、利用によって情報を書き換える際には、更新データを修正属性ＡＴ２，ＡＴ３，．．．の形でエニーキャスト・アドレス情報に追加する。これらの修正属性は、それぞれの修正を施した機器、すなわちユーザ端末、可搬型記憶媒体、あるいはエニーキャスト・アドレス設定処理装置が生成するディジタル署名とともにエニーキャスト・アドレス情報に追加される。エニーキャスト・アドレス情報は、エニーキャスト・アドレス設定処理装置、可搬型記憶媒体、ユーザ端末それぞれの間でやりとりされ、その都度、情報受信者が署名検証により改竄の有無を検査する。

【００７８】顧客（ユーザ）は購入したエニーキャスト・アドレスを、複数の可搬型記憶媒体にコピーすることで、ユーザの所有する様々な通信端末装置としての各種機器に振り分け、それらの間でエニーキャスト・アドレスを共有することができる。結果として、それらの機器の間でエニーキャスト・サービスが共有される。例えばメモリースティック端子を有するＡＶ機器に同一のエニーキャスト・アドレスを持つメモリースティックを装着することで、それらの間でエニーキャスト・サービスを行うことが出来る。コピー作業に用いる機器としてはユーザの所有するＰＣ、携帯電話、ＰＤＡ等の機器を用いることが出来る。

【００７９】また、ユーザはエニーキャスト・アドレスが不要になった場合、不要になったエニーキャスト・アドレスを書き込んだ可搬型記憶媒体を販売店に持ち込み、そこで不要なエニーキャスト・アドレスをエニーキャスト・アドレス設定処理装置を用いて可搬型記憶媒体から消去してもらう。この時、同時にエニーキャスト・アドレスと顧客情報その他の対応関係を可搬型記憶媒体、エニーキャスト・アドレス設定処理装置から消去する。

【００８０】以下、本発明のシステムにおいて実行される処理について、

（１）エニーキャスト・アドレス設定処理装置から可搬型記憶媒体に対するエニーキャスト・アドレスの発行処理、

（２）エニーキャスト・アドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスの移動処理

（３）エニーキャスト・アドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスのコピー処理

（４）エニーキャスト・アドレスの利用処理

（５）エニーキャスト・アドレス返却（回収）処理

以上、各処理の詳細について説明する。

【００８１】［（１）エニーキャスト・アドレス設定処理装置から可搬型記憶媒体に対するエニーキャスト・アドレスの発行処理］まず、エニーキャスト・アドレス設定処理装置から可搬型記憶媒体に対するエニーキャスト・アドレスの発行処理の詳細について説明する。図６にエニーキャスト・アドレス新規発行処理における処理シーケンスを説明する図を示す。ここでの可搬型記憶媒体は、工場から出荷後まだ使用されていない可搬型記憶媒体であり、可搬型記憶媒体のメモリには、エニーキャスト・アドレスが書き込まれていない。

【００８２】まず、可搬型記憶媒体と、エニーキャスト・アドレス設定処理装置間相互の通信プラグ、通信ソケットを接続する。接続がなされると、認証処理が実行される。認証処理は、通信を実行する機器相互が正当な機器であることの確認処理として実行される。認証処理としては、公開鍵認証方式、共通鍵認証方式、ＩＰｖ４で実績のあるＫｅｒｂｅｒｏｓと電子透かしを組み合わせる方法や、あるいは、ＳＤＭＩ（Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ Ｍｕｓｉｃ Ｉｎｉｔｉａｔｉｖｅ）が提唱するインタフェース仕様を設計し実装する方法などが採用可能である。

【００８３】認証処理の一例として、公開鍵認証方式の処理シーケンスを図７を用いて説明する。公開鍵暗号方式の実行のために、可搬型記憶媒体のＲＯＭには認証データとして、可搬型記憶媒体（Ｓｎ）の公開鍵Ｋｐｕｂ－Ｓｎ，秘密鍵Ｋｐｒｉ－Ｓｎ、公開鍵証明書ＣｅｒｔＳｎが格納され、一方、エニーキャスト・アドレス設定処理装置（Ｗ）には、公開鍵Ｋｐｕｂ－Ｗ，秘密鍵Ｋｐｒｉ－Ｗ、公開鍵証明書ＣｅｒｔＷが格納されている。

【００８４】図７において、まず、エニーキャスト・アドレス設定処理装置は乱数Ｒｂを発生させ、可搬型記憶媒体に送る。可搬型記憶媒体は、乱数Ｒａ，Ｋａを発生させ、公開鍵暗号方式において適用される楕円曲線Ｅ上でシステム共通の点（ベースポイント）であるＧとＫａを乗算してＶａを計算し、さらに自分の秘密鍵（ＫＰｒｉ Ｓｎ）を用いてデータＲａ||Ｒｂ||Ｖａに対して施した電子署名とともに、公開鍵証明書（ＣｅｒｔＳｎ）他のデータ（ＣｅｒｔＳｎ||Ｒａ||Ｒｂ||Ｖａ）をエニーキャスト・アドレス設定処理装置に送る。電子署名は一般的なディジタル署名技術、例えばＲＳＡ暗号とハッシュ関数ＳＨＡ－１を組み合わせて実現するメッセージ・ダイジェスト方式などを用いる。

【００８５】エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の公開鍵証明書（ＣｅｒｔＳｎ）の正当性、および署名の正当性を検査する。正当性が確認された場合は、エニーキャスト・アドレス設定処理装置は、乱数Ｋｂを生成して、公開鍵証明書他のデータ（ＣｅｒｔＷ||Ｒｂ||Ｒａ||Ｖｂ）とともに自分の秘密鍵（ＫＰｒｉ Ｗ）を用いてデータＲｂ||Ｒａ||Ｖｂに対して施した署名データを可搬型記憶媒体に送る。

【００８６】この後、可搬型記憶媒体では、エニーキャスト・アドレス設定処理装置の公開鍵証明書（ＣｅｒｔＷ）の正当性、および署名の正当性を検査する。正当性が確認された場合は、ＫａとＶｂを、エニーキャスト・アドレス設定処理装置ではＫｂとＶａを、それぞれ楕円曲線Ｅ上で乗算してセッションキーＫｓを得る。上述のような手法により、エニーキャスト・アドレス設定処理装置と可搬型記憶媒体で相互認証がなされ、その後のデータ通信で適用する暗号鍵としてのセッションキーＫｓを共有することができる。

【００８７】図６に戻り、エニーキャスト・アドレス新規発行処理シーケンスについて説明を続ける。図７で説明したような相互認証処理において、相互が正当な機器であることが確認されると、次に、エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレス情報（ＡＩ）生成処理を実行し、生成したエニーキャスト・アドレス情報（ＡＩ）に対して、自己の秘密鍵Ｋｐｒｉ－Ｗによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵Ｋｐｕｂ－Ｓｎによって暗号化して可搬型記憶媒体に送信する。なお、この例では、相互の機器間のデータ通信において、相手の公開鍵を暗号化処理用の鍵として適用した例を説明するが、公開鍵暗号方式における相互認証時に共有したセッション鍵を用いて通信データの暗号化を行なう構成としてもよい。

【００８８】暗号化されたエニーキャスト・アドレス情報を受信した可搬型記憶媒体は、受信データを自己の秘密鍵Ｋｐｒｉ－Ｓｎで復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証をエニーキャスト・アドレス設定処理装置の公開鍵Ｋｐｕｂ－Ｗを適用して行ない、改竄の有無を判定する。なお、ここでは電子署名は、エニーキャスト・アドレス設定処理装置の秘密鍵によってなされている例として説明しているが、他のＩＤ発行機関の秘密鍵によって署名がなされている構成としてもよく、この場合、署名検証を実行する可搬型記憶媒体には、署名検証のためのＩＤ発行機関の公開鍵を格納する。

【００８９】可搬型記憶媒体は、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２０の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。エニーキャスト・アドレス設定処理装置が受信確認応答を受信して、処理が終了する。

【００９０】［（２）エニーキャスト・アドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスの移動処理］次に、エニーキャスト・ア

ドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスの移動処理について、図８を参照して説明する。

【００９１】異なる可搬型記憶媒体間のエニーキャスト・アドレスの移動処理においては、エニーキャスト・アドレスの使用を停止しアドレスを出力するアドレス出力元可搬型記憶媒体８０１と、エニーキャスト・アドレスを新規に格納して使用を開始するアドレス出力先可搬型記憶媒体８０２とが、順次エニーキャスト・アドレス設定処理装置に接続されて処理が実行される。

【００９２】アドレス出力元可搬型記憶媒体８０１のメモリ（図３におけるインタフェースＩＤ格納メモリ３２４）には、電子署名の付加されたエニーキャスト・アドレス情報が書き込まれている。

【００９３】まず、エニーキャスト・アドレスの使用を停止しアドレスを出力するアドレス出力元可搬型記憶媒体８０１とエニーキャスト・アドレス設定処理装置相互間を接続し、相互認証処理を実行する。認証処理としては、前述したように、公開鍵認証方式、共通鍵認証方式、ＩＰｖ４で実績のあるＫｅｒｂｅｒｏｓと電子透かしを組み合わせる方法や、あるいは、ＳＤＭＩ（Ｓｅｃｕｒｅ ＤｉｇｉｔａｌＭｕｓｉｃ Ｉｎｉｔｉａｔｉｖｅ）が提唱するインタフェース仕様を設計し実装する方法などが採用可能である。

【００９４】相互認証処理において、相互が正当な機器であることが確認されると、次に、アドレス出力元可搬型記憶媒体８０１は、アドレス出力元可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキー、あるいは通信相手であるエニーキャスト・アドレス設定処理装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報としてエニーキャスト・アドレス設定処理装置に送信する。

【００９５】エニーキャスト・アドレス設定処理装置は、アドレス出力元可搬型記憶媒体８０１から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、アドレス出力元可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。さらに、属性検証処理を行なう。

【００９６】署名検証および属性検証処理の手順について図９を用いて説明する。まず、署名検証、属性検証処理を実行するデータ受信者はエニーキャスト・アドレス情報を受け取ると、最初にステップＳ１０１において、エニーキャスト・アドレス（図５、ＡＡ）に関して電子署名の検証を行なう。検証者はエニーキャスト・アドレスの生成者の公開鍵を予め取得しておくものとする。Ｓ１０２において、署名の検証でエラーとなれば、エニーキャスト・アドレスＡＡは改竄されたものと判定し、ステップＳ１１１でエニーキャスト・アドレスに何らかの処理を施して使用を禁止する。例えば、可搬型記憶媒体にアドレスの消去コマンドを送信し、消去処理を行なう。

【００９７】ステップＳ１０１におけるエニーキャスト・アドレスＡＡに関する電子署名の検証において、データ改竄なしと判定（Ｓ１０２でＹｅｓ）された場合は、ステップＳ１０３に進み、初期属性(図５、ＡＴ１)に関して電子署名の正当性を調べる。これも先と検証者は、属性付与者の公開鍵を取得しておく。ここで証明検証に適用する公開鍵はエニーキャスト・アドレス情報の発行人と同じである場合、異なる場合がある。Ｓ１０４において、署名の検証でエラーとなれば、初期属性ＡＴ１は改竄されたものと判定し、ステップＳ１１１でエニーキャスト・アドレスに何らかの処理を施して使用を禁止する。この実現例では消去する。

【００９８】次にステップＳ１０５において、さらに検証すべき修正属性が存在するかどうかを調べる。前述したように、エニーキャスト・アドレスＡＡのコピー、利用によって属性の更新が必要となる場合には、更新データを修正属性ＡＴ２，ＡＴ３，．．．の形でエニーキャスト・アドレス情報に追加する。これらの修正属性は、それぞれの修正を施した機器、すなわちユーザ端末、可搬型記憶媒体、あるいはエニーキャスト・アドレス設定処理装置が生成するディジタル署名とともにエニーキャスト・アドレス情報に追加される。ステップＳ１０５では、このような修正属性の有無を判定する。修正属性が無い場合は、すべての署名検証は終了し、ステップＳ１１０において、エニーキャスト・アドレス情報が正当であると判定して処理を終了する。

【００９９】修正属性が有る場合は、ステップＳ１０６に進み、検証を行なっていない修正属性の署名検証を実行する。修正の古い順（追加された順）に属性値を読み出し一連の検査を行なう。検査内容は、１）署名が正しいか（Ｓ１０７）、２）コピー回数が増える修正が存在しないかどうか（Ｓ１０８）、３）利用可能時間が増える修正が存在しないかどうか（Ｓ１０９）、である。本実現例では、コピー回数と利用可能時間が減る使い方のみを実現するため、前述したチェックを行なうが、そうでなければ別のチェックを行なう。これらの検査を全ての修正属性に対して修正順に行なう。以上の全ての検査に成功すれば検査が終了するが、１つ以上の検査に失敗した場合は、Ｓ１１１において、そのエニーキャスト・アドレス情報に何らかの処理を施して使用を禁止する。この実現例では消去する。

【０１００】図８に戻り、異なる可搬型記憶媒体間のエニーキャスト・アドレスの移動処理のシーケンスについて説明を続ける。エニーキャスト・アドレス設定処理装置は、アドレス出力元可搬型記憶媒体８０１から受信したエニーキャスト・アドレス情報の署名検証等により、

データの正当性が確認されると、受信確認応答をアドレス出力元可搬型記憶媒体８０１に送信し、アドレス出力元可搬型記憶媒体８０１は確認応答に基づいて、エニーキャスト・アドレスの消去処理を行なう。

【０１０１】次に、エニーキャスト・アドレス設定処理装置では、アドレス出力先可搬型記憶媒体８０２を接続する。接続がなされると、認証処理が実行される。認証処理は、通信を実行する機器相互が正当な機器であることの確認処理として実行される。認証処理としては、公開鍵認証方式、共通鍵認証方式、ＩＰｖ４で実績のあるＫｅｒｂｅｒｏｓと電子透かしを組み合わせる方法や、あるいは、ＳＤＭＩ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ　Ｍｕｓｉｃ　Ｉｎｉｔｉａｔｉｖｅ）が提唱するインタフェース仕様を設計し実装する方法などが採用可能である。

【０１０２】例えば、図７で説明したような相互認証処理において、相互が正当な機器であることが確認されると、次に、エニーキャスト・アドレス設定処理装置は、アドレス出力元可搬型記憶媒体８０１から受信したエニーキャスト・アドレス情報に対して、自己の秘密鍵Ｋｐｒｉ－Ｗによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵Ｋｐｕｂ－Ｓｎによって暗号化してアドレス出力先可搬型記憶媒体８０２に送信する。なお、この例では、相互の機器間のデータ通信において、相手の公開鍵を暗号化処理用の鍵として適用した例を説明するが、公開鍵暗号方式における相互認証時に共有したセッション鍵を用いて通信データの暗号化を行なう構成としてもよい。

【０１０３】暗号化されたエニーキャスト・アドレス情報を受信したアドレス出力先可搬型記憶媒体８０２は、受信データを自己の秘密鍵Ｋｐｒｉ－Ｓｎで復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証をエニーキャスト・アドレス設定処理装置の公開鍵Ｋｐｕｂ－Ｗを適用して行ない、改竄の有無を判定する。なお、ここでは電子署名は、エニーキャスト・アドレス設定処理装置の秘密鍵によってなされている例として説明しているが、他のＩＤ発行機関の秘密鍵によって署名がなされている構成としてもよく、この場合、署名検証を実行する可搬型記憶媒体には、署名検証のためのＩＤ発行機関の公開鍵を格納する。

【０１０４】可搬型記憶媒体は、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２０の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。エニーキャスト・アドレス設定処理装置が受信確認応答を受信して、処理が終了する。

【０１０５】［（３）エニーキャスト・アドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスのコピー処理］次に、エニーキャスト・アドレス設定処理装置を介した、異なる可搬型記憶媒体間のエニーキャスト・アドレスのコピー処理について、図１０を用いて説明する。エニーキャスト・アドレスのコピー元となるコピー元可搬型記憶媒体９０１と、エニーキャスト・アドレスをコピーにより格納して使用を開始するコピー先可搬型記憶媒体９０２，９０３…とが、順次エニーキャスト・アドレス設定処理装置に接続されて処理が実行される。

【０１０６】コピー元可搬型記憶媒体９０１のメモリ（図３におけるインタフェースＩＤ格納メモリ３２４）には、電子署名の付加されたエニーキャスト・アドレス情報が書き込まれている。

【０１０７】まず、エニーキャスト・アドレスのコピー元となるコピー元可搬型記憶媒体９０１とエニーキャスト・アドレス設定処理装置相互間を接続し、相互認証処理を実行する。相互認証処理において、相互が正当な機器であることが確認されると、次に、コピー元可搬型記憶媒体９０１は、可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキー、あるいは通信相手であるエニーキャスト・アドレス設定処理装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報としてエニーキャスト・アドレス設定処理装置に送信する。

【０１０８】エニーキャスト・アドレス設定処理装置は、コピー元可搬型記憶媒体９０１から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。

【０１０９】エニーキャスト・アドレス設定処理装置は、コピー元可搬型記憶媒体９０１から受信したエニーキャスト・アドレス情報の署名検証等により、データの正当性が確認されると、受信確認応答をコピー元可搬型記憶媒体９０１に送信し、さらに、受信し正当性の検証されたエニーキャスト・アドレス情報（ＡＩ）に基づいてコピーＡＩ－１、ＡＩ－２を生成する。

【０１１０】なお、コピーされたエニーキャスト・アドレス情報（ＡＩ－ｎ）には、新たな修正属性が（電子署名と共に）追加される。コピーの結果得られる全てのエニーキャスト・アドレスの最終的なコピー回数の合計値は、当然、最初にコピーの元となったエニーキャスト・アドレス情報の最新のコピー可能回数と等しくなるように制御されねばならない。こうして複数のエニーキャスト・アドレス情報ＡＩ－１，ＡＩ－２，．．．が得られる。

【０１１１】次に、エニーキャスト・アドレス設定処理装置では、アドレスコピー先のコピー先可搬型記憶媒体

９０２を接続する。接続がなされると、認証処理が実行され、認証処理において、相互が正当な機器であることが確認されると、エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレスのコピー（ＡＩ－２）に対して、自己の秘密鍵Ｋｐｒｉ－Ｗによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵によって暗号化してコピー先可搬型記憶媒体９０２に送信する。

【０１１２】暗号化されたエニーキャスト・アドレス情報を受信したコピー先可搬型記憶媒体９０２は、受信データを自己の秘密鍵で復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証をエニーキャスト・アドレス設定処理装置の公開鍵Ｋｐｕｂ－Ｗを適用して行ない、改竄の有無を判定し、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２０の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。

【０１１３】さらに、エニーキャスト・アドレス設定処理装置では、アドレスコピー先のコピー先可搬型記憶媒体９０３を接続して同様の処理を繰り返す。これらの処理をコピー先となる可搬型記憶媒体の数に応じて繰り返し実行する。

【０１１４】［（４）エニーキャスト・アドレスの利用処理］次に、エニーキャスト・アドレスの利用処理について、図１１を用いて説明する。実際にユーザがＩＰｖ６通信を行なうときには通信端末装置としてのユーザ端末とエニーキャスト・アドレスを格納した可搬型記憶媒体の間で一時的なアドレスの授受が行なわれる。一時的、と書いた理由は、ＩＰｖ６通信利用時に限り可搬型記憶媒体がユーザ端末にエニーキャスト・アドレスを渡し可搬型記憶媒体から消去し、ＩＰｖ６通信が終了した後でユーザ端末は利用状況に応じてエニーキャスト・アドレス情報に修正属性を加え、そして可搬型記憶媒体に返却する処理を実行するからである。こうすることで同一のエニーキャスト・アドレス情報に関する予期しない同時使用を防ぐ。

【０１１５】図１１を参照してエニーキャスト・アドレスの利用処理について説明する。エニーキャスト・アドレスの提供元となる可搬型記憶媒体のメモリ（図３におけるインタフェースＩＤ格納メモリ３２４）には、電子署名の付加されたエニーキャスト・アドレス情報が書き込まれている。可搬型記憶媒体と通信端末装置としてのユーザ端末は通信プラグ、通信ソケットにより接続されデータ転送可能な状態となっている。

【０１１６】まず、エニーキャスト・アドレスの提供元となる可搬型記憶媒体とエニーキャスト・アドレス利用端末としての通信端末装置間で相互認証処理を実行する。相互認証処理において、相互が正当な機器であることが確認されると、次に、通信端末装置は、可搬型記憶媒体にアドレス転送を要求する。可搬型記憶媒体は、可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキー、あるいは通信相手である通信端末装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報として通信端末装置に送信する。

【０１１７】通信端末装置は、可搬型記憶媒体から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、アドレス出力元可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。

【０１１８】さらに、通信端末装置は、可搬型記憶媒体から受信したエニーキャスト・アドレス情報の属性検証により、コピー回数、利用時間検証等を行なう。これらは先に図９を用いて説明したステップＳ１０８，Ｓ１０９と同様の処理である。データの正当性が確認されると、受信確認応答を可搬型記憶媒体に送信する。可搬型記憶媒体は確認応答に基づいて、エニーキャスト・アドレスの消去処理を行なう。

【０１１９】通信端末装置は、可搬型記憶媒体から受信したエニーキャスト・アドレス情報を自己のメモリ（図３におけるインタフェースＩＤ格納メモリ３１８）に格納し　自己のエニーキャスト・アドレスとして通信処理を開始する。なおこの際、ＩＰｖ６エニーキャスト・アドレスのように利用時間設定がなされている場合は、例えばＲＴＣを用いた利用時間計測を行なう。

【０１２０】通信処理が終了すると、計測された利用時間に基づいて、修正属性を生成し、さらに、自己の秘密鍵で署名を行なう。その後、可搬型記憶媒体の公開鍵によって暗号化して可搬型記憶媒体に送信する。

【０１２１】暗号化されたエニーキャスト・アドレス情報を受信した可搬型記憶媒体は、受信データを自己の秘密鍵で復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証を通信端末装置の公開鍵を適用して行ない、改竄の有無を判定し、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２０の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答を通信端末装置に送信して処理を終了する。

【０１２２】これらの処理により、可搬型記憶媒体に格納されるエニーキャスト・アドレス情報には通信端末装置の利用による修正属性が随時加えられて格納されることになる。

【０１２３】（５）エニーキャスト・アドレス返却

（回収）処理】次に、エニーキャスト・アドレス返却（回収）処理の詳細について説明する。図１２にエニーキャスト・アドレス返却（回収）処理における処理シーケンスを説明する図を示す。ここでの可搬型記憶媒体は、エニーキャスト・アドレスを返却する機器である。

【０１２４】可搬型記憶媒体のメモリには、電子署名の付加されエニーキャスト・アドレスが書き込まれている。エニーキャスト・アドレスの返却を行なう可搬型記憶媒体とエニーキャスト・アドレス設定処理装置間相互を接続し、相互認証処理を実行する。

【０１２５】相互認証処理において、相互が正当な機器であることが確認されると、次に、可搬型記憶媒体は、メモリに書き込まれたエニーキャスト・アドレスを読み出して、エニーキャスト・アドレス設定処理装置に送信する。エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体からエニーキャスト・アドレスを受信すると、電子署名の検証によるエニーキャスト・アドレスの改竄のないことの確認を条件として、エニーキャスト・アドレスの無効化処理として、エニーキャスト・アドレス管理データベースに登録されたデータの削除処理を実行する。エニーキャスト・アドレス管理データベースは、エニーキャスト・アドレスの発行管理用のデータベースであり、ユーザとエニーキャスト・アドレスの対応付けデータ、有効期限管理データ等を削除する。

【０１２６】その後、エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体に対してエニーキャスト・アドレス回収処理完了通知を送信し、完了通知を受信した可搬型記憶媒体は、自己のメモリに書き込まれたエニーキャスト・アドレスの消去処理を実行する。

【０１２７】なお、可搬型記憶媒体には、必要に応じて複数のエニーキャスト・アドレスを書き込むことが出来る。例えば、エニーキャスト・サービス等の異なるサービスを１つあるいは複数のＩＰｖ６機器で利用するために複数のエニーキャスト・アドレスを可搬型記憶媒体に格納し利用することが可能である。複数のエニーキャスト・アドレスを可搬型記憶媒体に保持することで、各エニーキャスト・アドレスに様々な品質・機能のサービスを関連付けることができる。例えばテレビ電話のアプリケーションサービスを適用するエニーキャスト・アドレスをエニーキャスト・アドレスとして可搬型記憶媒体に格納することで、ユーザ端末はエニーキャスト・アドレスXを用いてテレビ電話サービスも受けることが出来るようになる。

【０１２８】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２９】なお、明細書中において説明した一連の処理はハードウェア、ソフトウェア両者の複合構成によって実行することが可能である。ソフトウェアによる処理は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１３０】例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１３１】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【０１３２】

【発明の効果】以上、説明してきたように、本発明のアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムによれば、可搬型記憶媒体を用いてエニーキャスト・アドレスを配布することで、エニーキャスト・アドレスを様々な通信端末装置で利用可能とした。エニーキャスト・アドレスは機器の置き換えに対して不変となるので、電話等の可用性の高いサービスにＩＰｖ６通信を利用できるようになる。また、エニーキャスト・アドレスをユーザ固有の識別子として用いることが可能となり、顧客個別対応型サービスのインフラストラクチャとして有用となる。

【０１３３】さらに、エニーキャスト・アドレスの移動、コピー、返却等の処理が可能であり、アドレスの使いまわしを行うことができ、エニーキャスト・アドレスの効率的な利用が可能となる。また、エニーキャスト・アドレスのやり取りに必要な安全性をディジタルコンテンツ保護機構を用いて解決したことで、エニーキャスト・アドレスのやり取りを安全に出来るだけでなく、可搬

型記憶媒体に対応する一般機器で行うことが出来、ユーザの利便性が高まる。また、エニーキャスト・アドレスの書き込み処理等を人手で入力する作業を省くことが可能となり、正確でかつ簡単にエニーキャスト・アドレスを配布することができ、ユーザの利便性が高まる。

【０１３４】さらに、複数のエニーキャスト・アドレスを可搬型記憶媒体に保持することが出来るため、各エニーキャスト・アドレスに様々な品質・機能のサービスを関連付けることが出来る。これにより、高機能な通信端末装置に対して複数のエニーキャスト・サービスを行わせ、製品の差別化を行うことができる。例えばエニーキャスト・アドレスＡに音声電話を、エニーキャスト・アドレスＢにテレビ電話の属性を与えた場合、可搬型記憶媒体を用いて音声端末にアドレスＡを、テレビ電話端末にアドレスＡ，Ｂを配布するようなアドレス利用処理が可能となる。

【図面の簡単な説明】

【図１】ＩＰｖ６アドレスのフォーマットを説明する図である。

【図２】本発明のアドレス管理システムの概要を説明する図である。

【図３】本発明のアドレス管理システムにおけるユーザ端末、可搬型記憶媒体、とエニーキャスト・アドレス設定処理装置の構成を説明する図である。

【図４】本発明のアドレス管理システムにおける処理の具体例を説明する図である。

【図５】本発明のアドレス管理システムにおける可搬型記憶媒体に格納されるエニーキャスト・アドレス情報のデータ構成例を説明する図である。

【図６】本発明のアドレス管理システムにおける新規エニーキャスト・アドレス発行処理シーケンスを示す図である。

【図７】本発明のアドレス管理システムにおける認証処理シーケンスを示す図である。

【図８】本発明のアドレス管理システムにおけるエニーキャスト・アドレス移動処理シーケンスを示す図である。

【図９】本発明のアドレス管理システムにおける署名検証、属性検証処理を示すフロー図である。

【図１０】本発明のアドレス管理システムにおけるエニーキャスト・アドレスコピーシーケンスを示す図である。

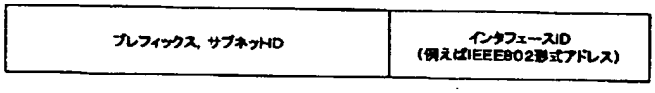
【図１１】本発明のアドレス管理システムにおけるエニーキャスト・アドレス利用処理シーケンスを示す図である。

【図１２】本発明のアドレス管理システムにおけるエニーキャスト・アドレス回収処理シーケンスを示す図である。

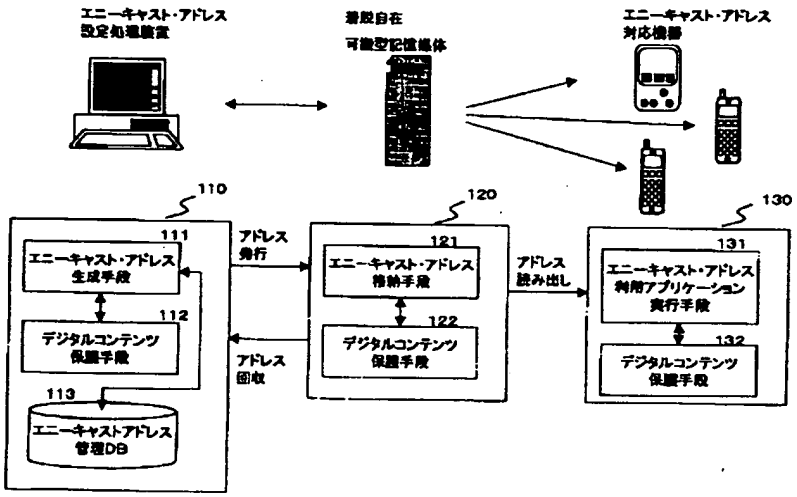
【符号の説明】

１１０　エニーキャスト・アドレス設定種理装置
１１１　エニーキャスト・アドレス生成手段
１１２　デジタルコンテンツ保護手段
１１３　エニーキャスト・アドレス管理データベース
１２０　可搬型記憶媒体
１２１　エニーキャスト・アドレス格納手段
１２２　デジタルコンテンツ保護手段
１３０　通信端末装置（ユーザ端末）
１３１　エニーキャスト・アドレス利用アプリケーション実行手段
１３２　デジタルコンテンツ保護手段
３１０　ユーザ端末
３１１　ＣＰＵ
３１２　ＲＯＭ
３１３　ＲＡＭ
３１４　入力部
３１５　出力部
３１６　ＩＰｖ６対応インタフェース
３１７　ＲＴＣ
３１８　インタフェースＩＤ格納メモリ
３１９　通信ソケット
３２０　可搬型記憶媒体
３２１　ＣＰＵ
３２２　ＲＯＭ
３２３　ＲＡＭ
３２４　インタフェースＩＤ格納メモリ
３２５　通信プラグ
３３０　エニーキャスト・アドレス設定処理装置
３３１　ＣＰＵ
３３２　ＲＯＭ
３３３　ＲＡＭ
３３４　入力部
３３５　出力部
３３６　エニーキャスト・アドレス管理データベース
３３７　通信ソケット
８０１　アドレス出力元可搬型記憶媒体
８０２　アドレス出力先可搬型記憶媒体
９０１　コピー元可搬型記憶媒体
９０２，９０２　コピー先可搬型記憶媒体

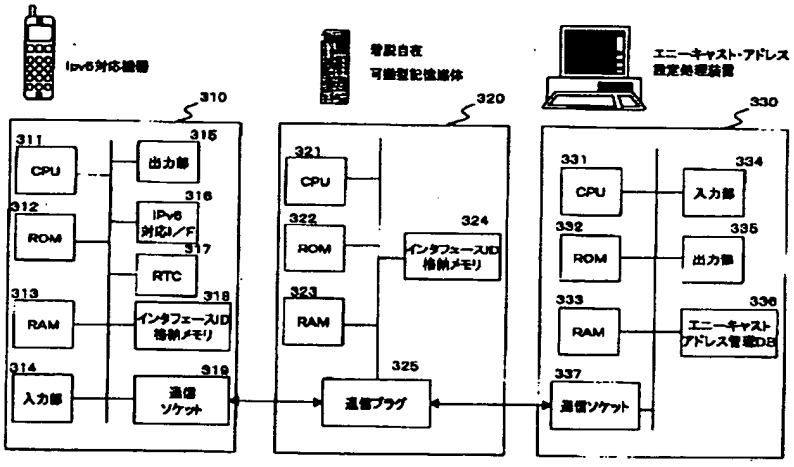
【図１】


プレフィックス、サブネットID
インタフェースID
（例えばIEEE802形式アドレス）

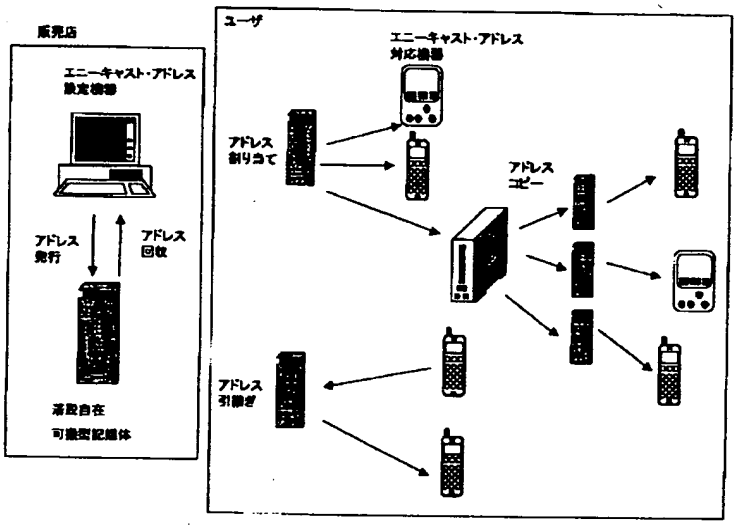
【図２】


エニーキャスト・アドレス
設定処理装置
着脱自在
可搬型記憶媒体
エニーキャスト・アドレス
対応機器
110
111
エニーキャスト・アドレス
生成手段
112
デジタルコンテンツ
保護手段
113
エニーキャストアドレス
管理DB
アドレス
発行
アドレス
回収
120
121
エニーキャスト・アドレス
格納手段
122
デジタルコンテンツ
保護手段
アドレス
読み出し
130
131
エニーキャスト・アドレス
利用アプリケーション
実行手段
132
デジタルコンテンツ
保護手段

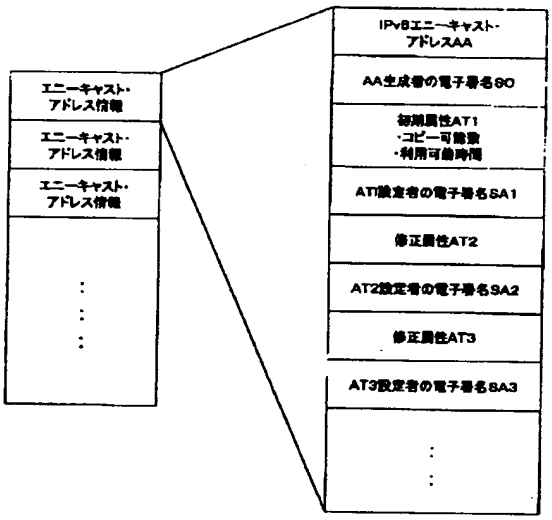
【図３】


Ipv6対応機器
着脱自在
可搬型記憶媒体
エニーキャスト・アドレス
設定処理装置
310
311
CPU
315
出力部
312
ROM
316
IPv6
対応I／F
317
RTC
313
RAM
318
インタフェースID
格納メモリ
314
入力部
319
通信
ソケット
320
321
CPU
322
ROM
324
インタフェースID
格納メモリ
323
RAM
325
通信プラグ
330
331
CPU
334
入力部
332
ROM
335
出力部
333
RAM
336
エニーキャスト
アドレス管理DB
337
通信ソケット

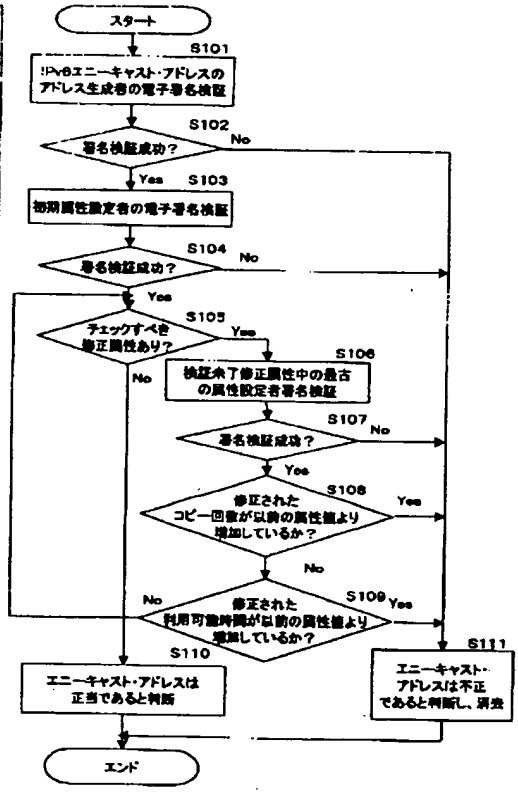
【図4】


販売店
エニーキャスト・アドレス
設定機器
アドレス
発行
アドレス
回収
端段自在
可搬型記録媒体
ユーザ
エニーキャスト・アドレス
対応機器
アドレス
割り当て
アドレス
コピー
アドレス
引継ぎ

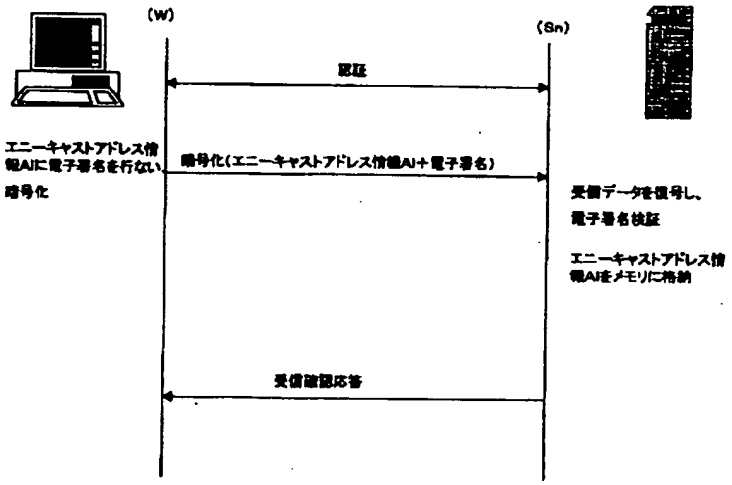
【図5】


エニーキャスト・
アドレス情報
エニーキャスト・
アドレス情報
エニーキャスト・
アドレス情報
IPv6エニーキャスト・
アドレスAA
AA生成者の電子署名SO
初期属性AT1
・コピー可能数
・利用可能時間
AT1設定者の電子署名SA1
修正属性AT2
AT2設定者の電子署名SA2
修正属性AT3
AT3設定者の電子署名SA3

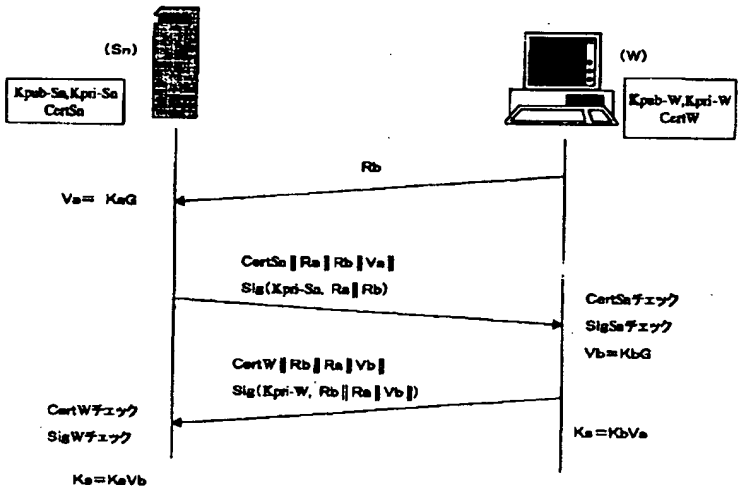
【図9】


スタート
S101
IPv6エニーキャスト・アドレスの
アドレス生成者の電子署名検証
S102
署名検証成功？
No
Yes
S103
初期属性設定者の電子署名検証
S104
署名検証成功？
No
Yes
S105
チェックすべき
修正属性あり？
Yes
No
S106
検証未了修正属性中の最古
の属性設定者署名検証
S107
署名検証成功？
No
Yes
S108
修正された
コピー回数が以前の属性値より
増加しているか？
Yes
No
S109
修正された
利用可能時間が以前の属性値より
増加しているか？
No
Yes
S110
エニーキャスト・アドレスは
正当であると判断
S111
エニーキャスト・
アドレスは不正
であると判断し、廃棄
エンド

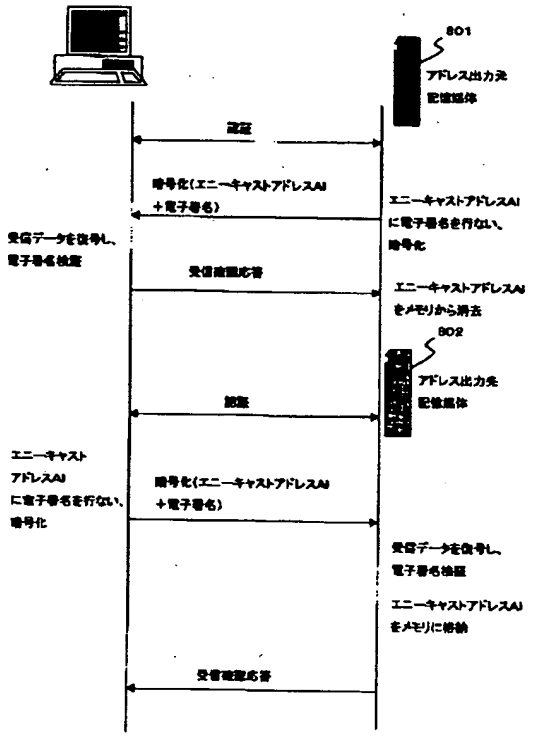
【図６】


(W)
(Sn)
認証
エニーキャストアドレス情報AIに電子署名を行ない
暗号化
暗号化(エニーキャストアドレス情報AI＋電子署名)
受信データを復号し、
電子署名検証
エニーキャストアドレス情報AIをメモリに格納
受信確認応答

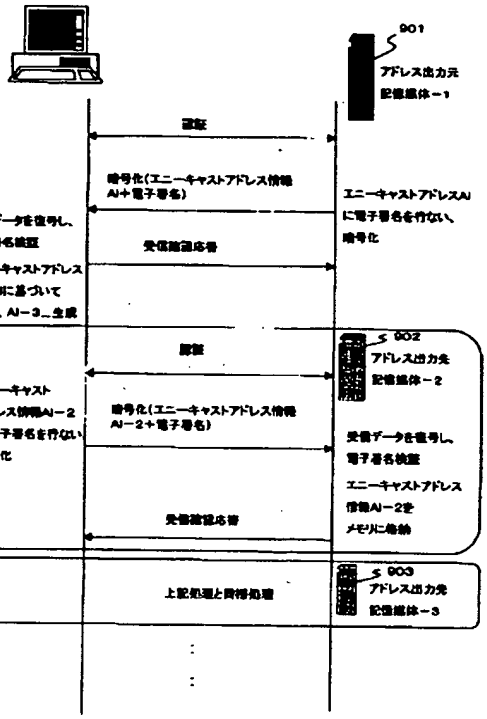
【図７】


(Sn)
Kpub-Sa,Kpri-Sa
CertSa
(W)
Kpub-W,Kpri-W
CertW
Rb
Va= KaG
CertSa‖Ra‖Rb‖Va‖
Sig(Kpri-Sa, Ra‖Rb)
CertSaチェック
SigSaチェック
Vb=KbG
CertW‖Rb‖Ra‖Vb‖
Sig(Kpri-W, Rb‖Ra‖Vb‖)
CertWチェック
SigWチェック
Ka=KbVa
Ka=KaVb

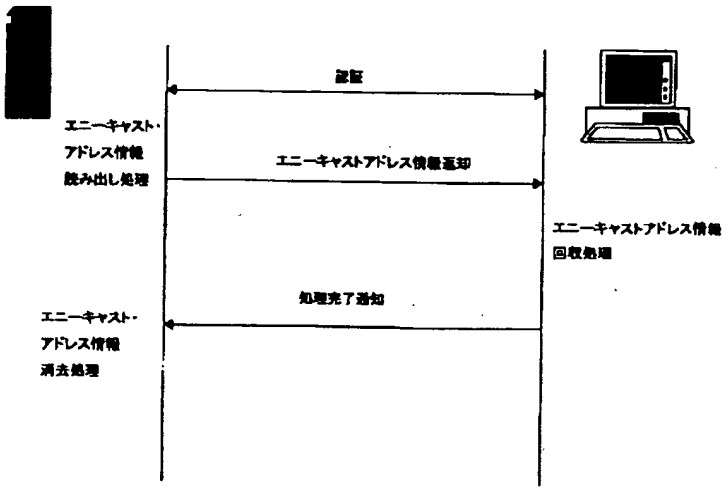
【図８】


801
アドレス出力元
記憶媒体
認証
暗号化(エニーキャストアドレスAI
＋電子署名)
エニーキャストアドレスAI
に電子署名を行ない、
暗号化
受信データを復号し、
電子署名検証
受信確認応答
エニーキャストアドレスAI
をメモリから消去
802
アドレス出力先
記憶媒体
認証
エニーキャスト
アドレスAI
に電子署名を行ない、
暗号化
暗号化(エニーキャストアドレスAI
＋電子署名)
受信データを復号し、
電子署名検証
エニーキャストアドレスAI
をメモリに格納
受信確認応答

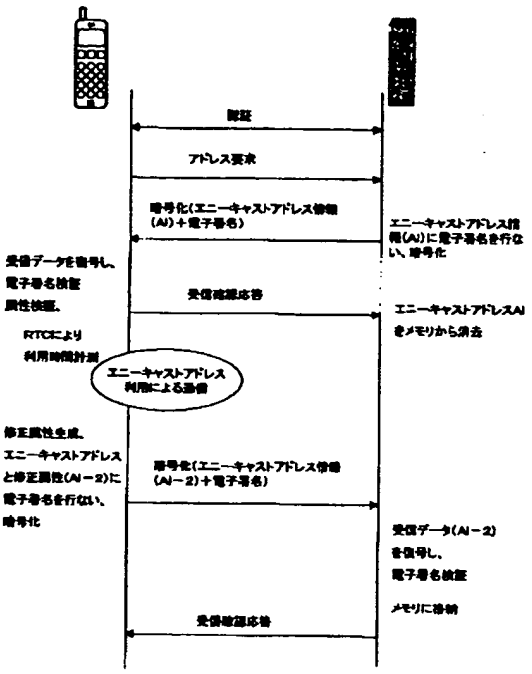
【図１０】


901
アドレス出力元
記憶媒体－1
認証
暗号化(エニーキャストアドレス情報
AI＋電子署名)
エニーキャストアドレスAI
に電子署名を行ない、
暗号化
受信データを復号し、
電子署名検証
受信確認応答
エニーキャストアドレス
情報AIに基づいて
AI－2, AI－3…生成
902
アドレス出力先
記憶媒体－2
認証
エニーキャスト
アドレス情報AI－2
に電子署名を行ない
暗号化
暗号化(エニーキャストアドレス情報
AI－2＋電子署名)
受信データを復号し、
電子署名検証
エニーキャストアドレス
情報AI－2を
メモリに格納
受信確認応答
903
アドレス出力先
記憶媒体－3
上記処理と同様処理

【図１２】


認証
エニーキャスト・
アドレス情報
読み出し処理
エニーキャストアドレス情報通知
エニーキャストアドレス情報
回収処理
処理完了通知
エニーキャスト・
アドレス情報
消去処理

【図１１】



フロントページの続き

Ｆターム(参考)　5B085 AE04 AE11 AE23 BG07
5K030 GA11 GA15 HA08 HB08 HD09
JT02 KA04

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１５年７月４日（２００３．７．４）

【公開番号】特開２００３－５１８３７（Ｐ２００３　５１８３７Ａ）
【公開日】平成１５年２月２１日（２００３．２．２１）
【年通号数】公開特許公報１５－５１９
【出願番号】特願２００１－２３９１４７（Ｐ２００１－２３９１４７）
【国際特許分類第７版】
　Ｈ０４Ｌ　１２/５６
// Ｇ０６Ｆ　１５/００　　３３０
【ＦＩ】
　Ｈ０４Ｌ　１２/５６　　Ｂ
　Ｇ０６Ｆ　１５/００　　３３０　Ｇ

【手続補正書】
【提出日】平成１５年３月２８日（２００３．３．２８）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正内容】
【００１３】本発明においては、デジタルコンテンツ保護機構を有する可搬型記憶装置を利用することで不正なＩＤ使用を防止しつつ面倒なＩＤ設定を簡単に行なうことのできるアドレス管理システム、エニーキャスト・アドレス設定処理装置、通信端末装置、情報格納装置、およびアドレス管理方法、並びにコンピュータ・プログラムを提供することを目的とする。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正内容】
【００２０】さらに、本発明のアドレス管理システムの一実施態様において、前記エニーキャスト・アドレス設定処理装置は、接続した第１の可搬型記憶媒体から受理した電子署名のなされたエニーキャスト・アドレス情報についての電子署名の検証によるエニーキャスト・アドレス情報の改竄のないことの確認を条件として、該エニーキャスト・アドレス情報を他の第２の可搬型記憶媒体に出力するエニーキャスト・アドレス情報の移動またはコピー処理を実行する構成を有することを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】変更
【補正内容】
【００６１】ＩＰｖ６対応インタフェース（Ｉ／Ｆ）３１６はＩＰｖ６プロトコルを用いて通信可能な通信路を提供する。接続サブネットのルータ等と通信し、ＣＰＵ３１１、ＲＡＭ３１５等から供給されたデータをパケット化して送信したり、パケットを受信する処理を実行する。ＲＴＣ３１７はエニーキャスト・アドレス情報に使用期限を設ける場合に使用するもので必須ではない。ＲＴＣはＩＰｖ６通信時間を計測する。その時に用いたエニーキャスト・アドレスに付随する使用可能時間から計測時間を減算して修正属性（後述）の形式でエニーキャスト・アドレス情報を更新するために使用する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００６３
【補正方法】変更
【補正内容】
【００６３】次に、可搬型記憶媒体３２０の構成について説明する。ＣＰＵ(Cntral processing Unit)３２１は、各種オペレーション、アプリケーションプログラムを実行する。具体的には、可搬型記憶媒体のメモリに対するデータ格納読み出し制御、データ暗号化、復号処理、署名生成、検証処理、ユーザ端末、あるいはエニーキャスト・アドレス設定処理装置間で実行されるエニーキャスト・アドレス送受信処理の制御、認証処理等を行なう。ＲＯＭ（Read-Only-Memory）３２２は、ＣＰＵ３２１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）３２３は、ＣＰＵ３２１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００７４
【補正方法】変更

【補正内容】
【００７４】販売店はエニーキャスト・アドレス設定処理装置を保有し、顧客がエニーキャスト・アドレスを購入するときにエニーキャスト・アドレス設定処理装置を用いて、顧客の可搬型記憶媒体にエニーキャスト・アドレスを書き込む。このとき同時に顧客に関する種々の情報を新規発行したエニーキャスト・アドレスと組み合わせてエニーキャスト・アドレス設定処理装置および可搬型記憶媒体に登録する。可搬型記憶媒体としては例えばメモリースティックなどのデジタルコンテンツ保護機構を有する機器である。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００７９
【補正方法】変更
【補正内容】
【００７９】また、ユーザはエニーキャスト・アドレスが不要になった場合、不要になったエニーキャスト・アドレスを書き込んだ可搬型記憶媒体を販売店に持ち込み、そこで不要なエニーキャスト・アドレスをエニーキャスト・アドレス設定処理装置を用いて可搬型記憶媒体から消去してもらう。この時、同時にエニーキャスト・アドレスと顧客情報その他の対応関係を可搬型記憶媒体、エニーキャスト・アドレス設定処理装置のアドレス管理ＤＢ３３６から消去する。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００８４
【補正方法】変更
【補正内容】
【００８４】図７において、まず、エニーキャスト・アドレス設定処理装置は乱数Ｒｂを発生させ、可搬型記憶媒体に送る。可搬型記憶媒体は、乱数Ｒａ、Ｋａを発生させ、公開鍵暗号方式において適用される楕円曲線Ｅ上でシステム共通の点（ベースポイント）であるＧとＫａを乗算してＶａを計算し、さらに自分の秘密鍵（ＫＰｒｉ－Ｓｎ）を用いてデータＲａ||Ｒｂ|Ｖａに対して施した電子署名（ＳｉｇＳｎ）とともに、公開鍵証明書（ＣｅｒｔＳｎ）他のデータ（ＣｅｒｔＳｎ||Ｒａ||Ｒｂ||Ｖａ）をエニーキャスト・アドレス設定処理装置に送る。電子署名は一般的なディジタル署名技術、例えばＲＳＡ暗号とハッシュ関数ＳＨＡ－１を組み合わせて実現するメッセージ・ダイジェスト方式などを用いる。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００８５
【補正方法】変更
【補正内容】
【００８５】エニーキャスト・アドレス設定処理装置は、可搬型記憶媒体の公開鍵証明書（ＣｅｒｔＳｎ）の正当性、および署名（ＳｉｇＳｎ）の正当性を検査する。正当性が確認された場合は、エニーキャスト・アドレス設定処理装置は、乱数Ｋｂを生成して、公開鍵証明書他のデータ（ＣｅｒｔＷ||Ｒｂ||Ｒａ||Ｖｂ）とともに自分の秘密鍵（ＫＰｒｉ－Ｗ）を用いてデータＲｂ||Ｒａ||Ｖｂに対して施した署名データ（ＳｉｇＷ）を可搬型記憶媒体に送る。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００８６
【補正方法】変更
【補正内容】
【００８６】この後、可搬型記憶媒体では、エニーキャスト・アドレス設定処理装置の公開鍵証明書（ＣｅｒｔＷ）の正当性、および署名（ＳｉｇＷ）の正当性を検査する。正当性が確認された場合は、ＫａとＶｂを、エニーキャスト・アドレス設定処理装置ではＫｂとＶａを、それぞれ楕円曲線Ｅ上で乗算してセッションキーＫｓを得る。上述のような手法により、エニーキャスト・アドレス設定処理装置と可搬型記憶媒体で相互認証がなされ、その後のデータ通信で適用する暗号鍵としてのセッションキーＫｓを共有することができる。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００８７
【補正方法】変更
【補正内容】
【００８７】図６に戻り、エニーキャスト・アドレス新規発行処理シーケンスについて説明を続ける。図７で説明したような相互認証処理において、相互が正当な機器であることが確認されると、次に、エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレス情報（ＡＩ）生成処理を実行し、生成したエニーキャスト・アドレス情報（ＡＩ）に対して、自己の秘密鍵ＫｐｒｉｅｒＷによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵Ｋｐｕｂ－Ｓｎによって暗号化して可搬型記憶媒体に送信する。なお、この例では、相互の機器間のデータ通信において、相手の公開鍵を暗号化処理用の鍵として適用した例を説明するが、公開鍵暗号方式における相互認証時に共有したセッションキーＫｓを用いて通信データの暗号化を行なう構成としてもよい。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００８９
【補正方法】変更
【補正内容】
【００８９】可搬型記憶媒体は、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示

すＣＰＵ３２１の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。エニーキャスト・アドレス設定処理装置が受信確認応答を受信して、処理が終了する。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００９４
【補正方法】変更
【補正内容】
【００９４】相互認証処理において、相互が正当な機器であることが確認されると、次に、アドレス出力元可搬型記憶媒体８０１は、アドレス出力元可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキーＫｓ、あるいは通信相手であるエニーキャスト・アドレス設定処理装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報としてエニーキャスト・アドレス設定処理装置に送信する。

【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００９５
【補正方法】変更
【補正内容】
【００９５】エニーキャスト・アドレス設定処理装置は、アドレス出力元可搬型記憶媒体８０１から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーＫｓあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、アドレス出力元可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。さらに、属性検証処理を行なう。

【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】０１０２
【補正方法】変更
【補正内容】
【０１０２】例えば、図７で説明したような相互認証処理において、相互が正当な機器であることが確認されると、次に、エニーキャスト・アドレス設定処理装置は、アドレス出力元可搬型記憶媒体８０１から受信したエニーキャスト・アドレス情報に対して、自己の秘密鍵Ｋｐｒｉ－Ｗによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵Ｋｐｕｂ－Ｓｎによって暗号化してアドレス出力先可搬型記憶媒体８０２に送信する。なお、この例では、相互の機器間のデータ通信において、相手の公開鍵を暗号化処理用の鍵として適用した例を説明するが、公開鍵暗号方式における相互認証時に共有したセッションキーＫｓを用いて通信データの暗号化を行なう構成としてもよい。

【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】０１０４
【補正方法】変更
【補正内容】
【０１０４】可搬型記憶媒体は、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２１の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。エニーキャスト・アドレス設定処理装置が受信確認応答を受信して、処理が終了する。

【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】０１０７
【補正方法】変更
【補正内容】
【０１０７】まず、エニーキャスト・アドレスのコピー元となるコピー元可搬型記憶媒体９０１とエニーキャスト・アドレス設定処理装置相互間を接続し、相互認証処理を実行する。相互認証処理において、相互が正当な機器であることが確認されると、次に、コピー元可搬型記憶媒体９０１は、可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキーＫｓ、あるいは通信相手であるエニーキャスト・アドレス設定処理装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報としてエニーキャスト・アドレス設定処理装置に送信する。

【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】０１０８
【補正方法】変更
【補正内容】
【０１０８】エニーキャスト・アドレス設定処理装置は、コピー元可搬型記憶媒体９０１から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーＫｓあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。

【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】０１０９
【補正方法】変更
【補正内容】
【０１０９】エニーキャスト・アドレス設定処理装置は、コピー元可搬型記憶媒体９０１から受信したエニーキャスト・アドレス情報の署名検証等により、データの

正当性が確認されると、受信確認応答をコピー元可搬型記憶媒体９０１に送信し、さらに、受信し正当性の検証されたエニーキャスト・アドレス情報（ＡＩ）に基づいてコピーＡＩ－１，ＡＩ－２を生成する。受信確認応答を受け取ったコピー元過般型記憶媒体９０１はエニーキャストアドレス情報（ＡＩ）をメモリ３２４から消去する。

【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】０１１１
【補正方法】変更
【補正内容】
【０１１１】次に、エニーキャスト・アドレス設定処理装置では、アドレスコピー先のコピー先可搬型記憶媒体９０２を接続する。接続がなされると、認証処理が実行され、認証処理において、相互が正当な機器であることが確認されると、エニーキャスト・アドレス設定処理装置は、エニーキャスト・アドレスのコピー（ＡＩ－２）に対して、自己の秘密鍵Ｋｐｒｉ－Ｗあるいはセッションキー－Ｋｓによって電子署名を施し、さらに、先の認証処理の際に取得した可搬型記憶媒体の公開鍵によって暗号化してコピー先可搬型記憶媒体９０２に送信する。

【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】０１１２
【補正方法】変更
【補正内容】
【０１１２】暗号化されたエニーキャスト・アドレス情報を受信したコピー先可搬型記憶媒体９０２は、受信データを自己の秘密鍵で復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証をエニーキャスト・アドレス設定処理装置の公開鍵Ｋｐｕｂ－Ｗあるいはセッションキー－Ｋｓを適用して行ない、改竄の有無を判定し、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２０の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答をエニーキャスト・アドレス設定処理装置に送信する。

【手続補正２１】
【補正対象書類名】明細書
【補正対象項目名】０１１６
【補正方法】変更
【補正内容】
【０１１６】まず、エニーキャスト・アドレスの提供元となる可搬型記憶媒体とエニーキャスト・アドレス利用端末としての通信端末装置間で相互認証処理を実行する。相互認証処理において、相互が正当な機器であることが確認されると、次に、通信端末装置は、可搬型記憶媒体にアドレス転送を要求する。可搬型記憶媒体は、可搬型記憶媒体内のメモリに書き込まれたエニーキャスト・アドレス情報を読み出して、自己の秘密鍵による署名を生成し、さらに、セッションキーＫｓ、あるいは通信相手である通信端末装置の公開鍵を用いて送信データの暗号化処理を実行し、署名付き暗号化エニーキャスト・アドレス情報として通信端末装置に送信する。

【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】０１１７
【補正方法】変更
【補正内容】
【０１１７】通信端末装置は、可搬型記憶媒体から暗号化されたエニーキャスト・アドレス情報を受信すると、セッションキーＫｓあるいは自己の秘密鍵を適用して復号処理を行ない、さらに、アドレス出力元可搬型記憶媒体の公開鍵を適用して署名検証を実行しデータ改竄の有無をチェックする。

【手続補正２３】
【補正対象書類名】明細書
【補正対象項目名】０１２１
【補正方法】変更
【補正内容】
【０１２１】暗号化されたエニーキャスト・アドレス情報を受信した可搬型記憶媒体は、受信データを自己の秘密鍵で復号処理を行なった後、エニーキャスト・アドレス情報に対する電子署名の検証を通信端末装置の公開鍵を適用して行ない、改竄の有無を判定し、署名検証によりエニーキャスト・アドレス情報に改竄が無いと判定すると、電子署名を含むエニーキャスト・アドレス情報を図３に示すＣＰＵ３２１の制御のもとにインタフェースＩＤ格納メモリ３２４に格納する。これらの処理の後、可搬型記憶媒体は、受信確認応答を通信端末装置に送信して処理を終了する。

【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】０１２７
【補正方法】変更
【補正内容】
【０１２７】なお、可搬型記憶媒体には、必要に応じて複数のエニーキャスト・アドレスを書き込むことが出来る。例えば、エニーキャスト・サービス等の異なるサービスを１つあるいは複数のＩＰｖ６機器で利用するために複数のエニーキャスト・アドレスを可搬型記憶媒体に格納し利用することが可能である。複数のエニーキャスト・アドレスを可搬型記憶媒体に保持することで、各エニーキャスト・アドレスに様々な品質・機能のサービスを関連付けることができる。例えばテレビ電話のアプリケーションサービスを適用するエニーキャスト・アドレスＸをエニーキャスト・アドレスとして可搬型記憶媒体

に格納することで、ユーザ端末はエニーキャスト・アドレスＸを用いてテレビ電話サービスも受けることが出来るようになる。

【手続補正２５】
【補正対象書類名】明細書
【補正対象項目名】０１３３
【補正方法】変更
【補正内容】
【０１３３】さらに、エニーキャスト・アドレスの移動、コピー、返却等の処理が可能であり、アドレスの使いまわしを行うことができ、エニーキャスト・アドレスの効率的な利用が可能となる。また、エニーキャスト・アドレスのやり取りに必要な安全性をデジタルコンテン＊ツ保護機構を用いて解決したことで、エニーキャスト・アドレスのやり取りを安全に出来るだけでなく、可搬型記憶媒体に対応する一般機器で行うことが出来、ユーザの利便性が高まる。また、エニーキャスト・アドレスの書き込み処理等を人手で入力する作業を省くことが可能となり、正確でかつ簡単にエニーキャスト・アドレスを配布することができ、ユーザの利便性が高まる。

【手続補正２６】
【補正対象書類名】図面
【補正対象項目名】図１０
【補正方法】変更
【補正内容】
【図１０】